802.11 b/g/n

Micro Mini Wireless LAN

USB2.0 Adapter

WN2000

User's Manual

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

Country Code Statement

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

To maintain compliance with FCC RF exposure requirements, use only belt-clips, holsters or similar accessories that do not contain metallic components in its assembly. The use of accessories that do not satisfy these requirements may not comply with FCC RF exposure requirements, and should be avoided.

CAUTION:
Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Federal Communication Commission (FCC) Radiation Exposure Statement

This EUT is compliance with SAR for general population/uncontrolled exposure limits in ANSI/IEEE C95.1-1999 and had been tested in accordance with the measurement methods and procedures specified in OET Bulletin 65 Supplement C. This equipment should be installed and operated with minimum distance 2.5cm between the radiator & your body.

CE Statement:

Hereby, AboCom, declares that this device is in compliance with the essential requirement and other relevant provisions of the R&TTE Driective 1999/5/EC.

Table of Contents

INTRODUCTION 1

FEATURES 1

Windows 2000/XP Installation 2

INSTALL THE SOFTWARE 2

INSTALL THE HARDWARE 5

Windows Vista Installation 6

INSTALL THE SOFTWARE 6

INSTALL THE HARDWARE 8

VERIFICATION 8

NETWORK CONNECTION 9

IP ADDRESS 9

UTILITY CONFIGURATION FOR WINDOWS 2000/XP 10

STATION MODE 11

Profile 11

Network 20

Link Status 23

Advanced 25

Statistics 27

WMM / QoS 28

WPS 30
Radio On/Off 33
About 34
UTILITY MENU LIST 35
SOFT AP MODE 36
Config 36
Access Control 39
MAC Table 40
Event Log 41
Statistics 42
About 43
UTILITY CONFIGURATION FOR WINDOWS VISTA 44
STATION MODE 45
Profile 45
Network 53
Link Status 57
Advanced 59
Statistics 60
WMM / QoS 62
WPS 63
Radio On/Off 66
About 67
UTILITY MENU LIST 67

SOFT AP MODE 68
Config 68
Access Control 71
MAC Table 72
Event Log 73
Statistics 74
About 75
UNINSTALLATION FOR WINDOWS 2000/XP 76
UNINSTALLATION FOR WINDOWS VISTA 78

INTRODUCTION

The **WN2000** is an IEEE802.11b/g/n USB adapter that connects your notebook to a wireless local area. The **WN2000** fully complies with IEEE 802.11n draft 3.0 and IEEE 802.11 b/g standards, delivers reliable, cost-effective, feature rich wireless connectivity at high throughput from an extended distance.

The **WN2000** is a very small adapter that can connects notebook, handheld or desktop computer equipped with USB interface for wireless network applications. It allows you to take full advantage of your notebook's mobility with access to real-time information and online services anytime and anywhere.

Features

- 1T1R Mode with 150Mbps PHY Rate for both.
- Complies with IEEE 802.11n draft 3.0 and IEEE 802.11 b/g standards.
- Supports WEP 64/128, WPA, WPA2.
- Supports WMM and WMM-PS.
- Supports WPS configuration.
- Supports USB 2.0/1.1 interface.
- Portable and mini-size design.
- Compatible with Microsoft Windows Vista, XP, 2000.

Windows 2000/XP Installation

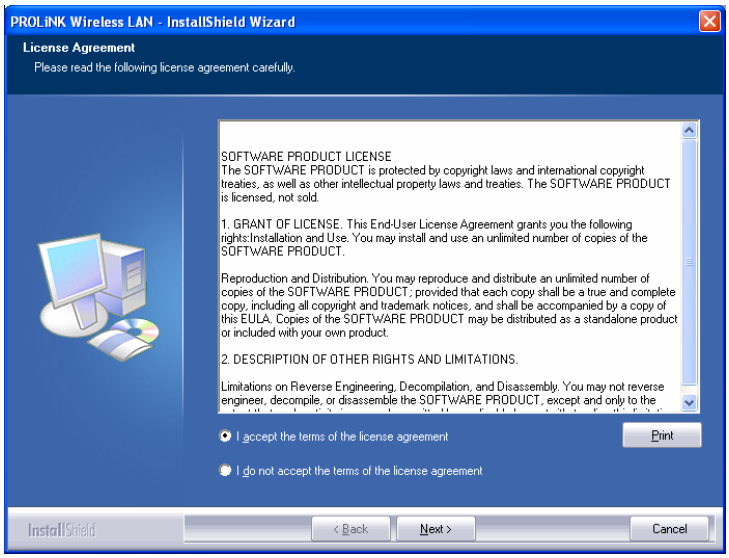
Install the Software

Caution!

Do not insert the wireless card into your computer until the InstallShield Wizard finish installing.

1. Exit all Windows programs. Insert the included CD-ROM into your computer. The CD-ROM will run automatically.

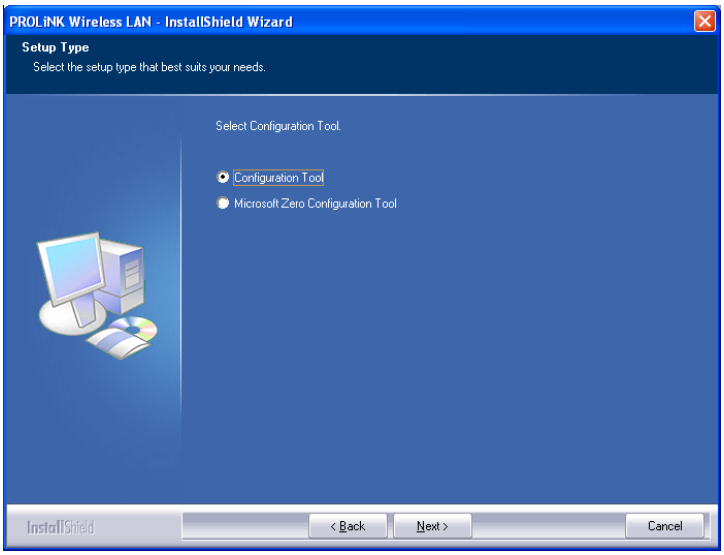
2. When the License Agreement screen appears, please read the contents and select "**I accept the terms of the license agreement** " then click **Next** to continue.


PROLiNK Wireless LAN - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
SOFTWARE PRODUCT LICENSE
The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.
1. GRANT OF LICENSE. This End-User License Agreement grants you the following rights:Installation and Use. You may install and use an unlimited number of copies of the SOFTWARE PRODUCT.
Reproduction and Distribution. You may reproduce and distribute an unlimited number of copies of the SOFTWARE PRODUCT; provided that each copy shall be a true and complete copy, including all copyright and trademark notices, and shall be accompanied by a copy of this EULA. Copies of the SOFTWARE PRODUCT may be distributed as a standalone product or included with your own product.
2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.
Limitations on Reverse Engineering, Decompilation, and Disassembly. You may not reverse engineer, decompile, or disassemble the SOFTWARE PRODUCT, except and only to the
I accept the terms of the license agreement
I do not accept the terms of the license agreement
Print
InstallShield
< Back
Next >
Cancel

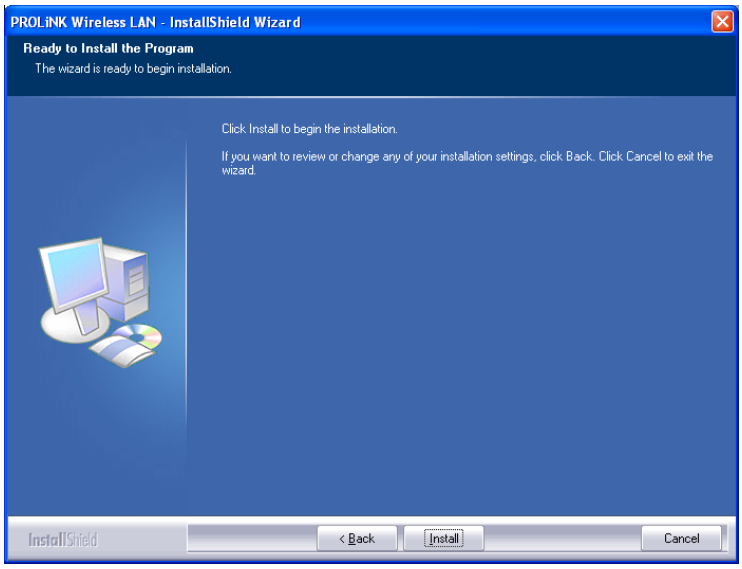
3. Select the check box to choose a **Configuration Tool** from the listed two choices.

   - **Configuration Tool**: Choose to use our configuration utility.
   - **Microsoft Zero Configuration Tool**: Choose to use Windows XP's built-in Zero Configuration Utility (ZCU).

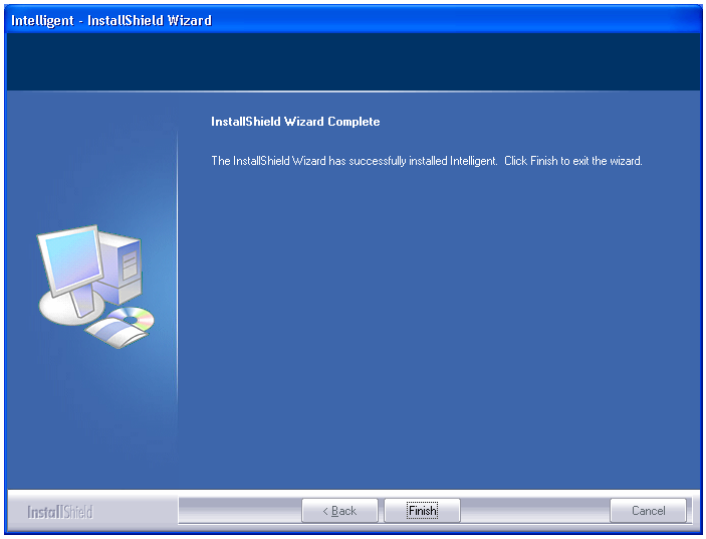
   Click **Next** to continue.



5. When you are prompted the following message, please click **Install** to begin the installation.


PROLiNK Wireless LAN - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

6. When the following screen appears, click **Finish** to complete the software installation.



Install the Hardware

Note: Insert the Wireless USB card when you finished your software installation.

Insert the USB Adapter into the USB Port of your computer. The system will automatically detect the new hardware.

Windows Vista Installation

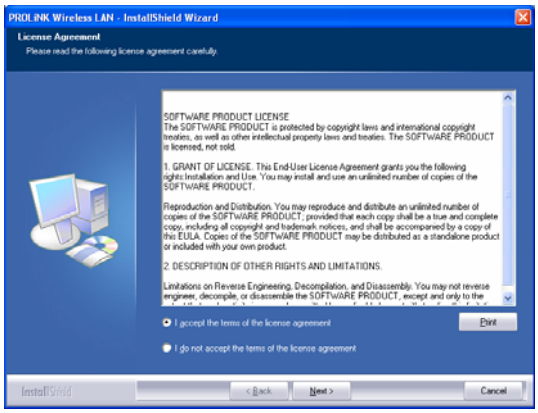
Install the Software

Do not insert the wireless LAN adapter into your computer until the procedures in "Driver& Utility Installation" have been performed.

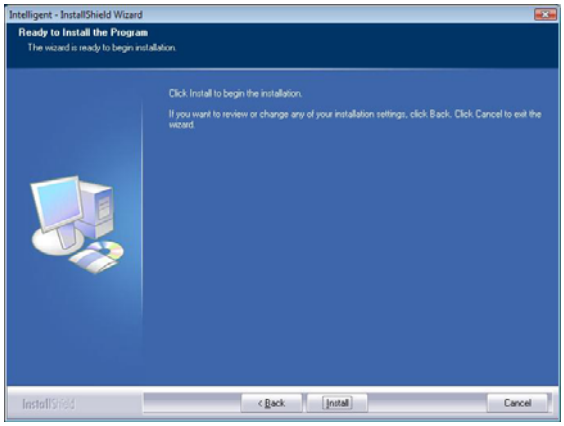
1. Insert the included CD-ROM into the CD-ROM drive of your computer.

2. When the Main Menu screen appears, click "**Driver & Utility Installation**" to start the software installation.

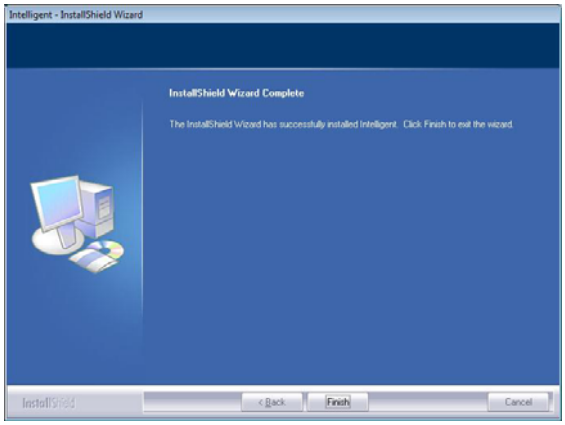
3. When the **License Agreement** screen appears, please read the contents and select "**I accept the terms of the license agreement** " then click **Next** to continue.


PROLiNK Wireless LAN - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
SOFTWARE PRODUCT LICENSE
The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.
1. GRANT OF LICENSE. This End-User License Agreement grants you the following rights: Installation and Use. You may install and use an unlimited number of copies of the SOFTWARE PRODUCT.
Reproduction and Distribution. You may reproduce and distribute an unlimited number of copies of the SOFTWARE PRODUCT; provided that each copy shall be a true and complete copy, including all copyright and trademark notices, and shall be accompanied by a copy of this EULA. Copies of the SOFTWARE PRODUCT may be distributed as a standalone product or included with your own product.
2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.
Limitations on Reverse Engineering, Decompilation, and Disassembly. You may not reverse engineer, decompile, or disassemble the SOFTWARE PRODUCT, except and only to the
I accept the terms of the license agreement
I do not accept the terms of the license agreement
Print
InstallShield
< Back
Next >
Cancel

4. When you are prompted the following message, please click **Install** to begin the installation.


Intelligent - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

5. When the following screen appears, click **Finish** to complete the software installation.



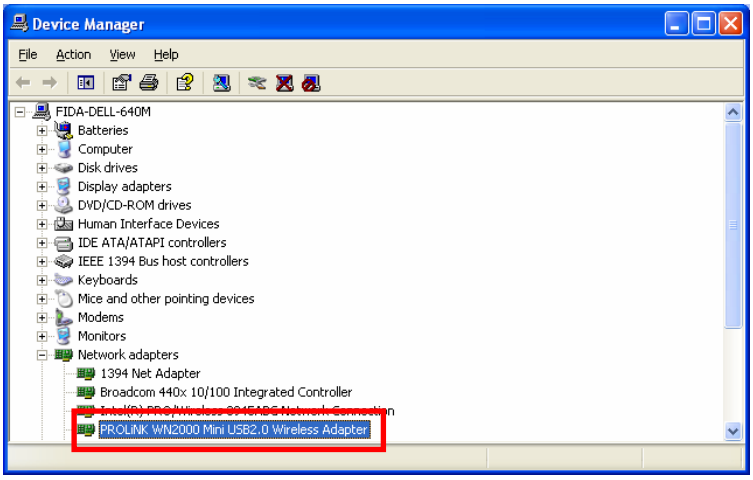
Install the Hardware

Note: Insert the Wireless USB card when you finished your software installation.

Insert the USB Adapter into the USB Port of your computer. The system will automatically detect the new hardware.

Verification

To verify if the device exists in your computer and is enabled, go to **Start** > **Control Panel** > **System** > **Hardware** > **Device Manager**. Expand the **Network Adapters** category. If the **PROLiNK WN2000 Mini USB2.0 Wireless Adapter** is listed here, it means that your device is properly installed and enabled.



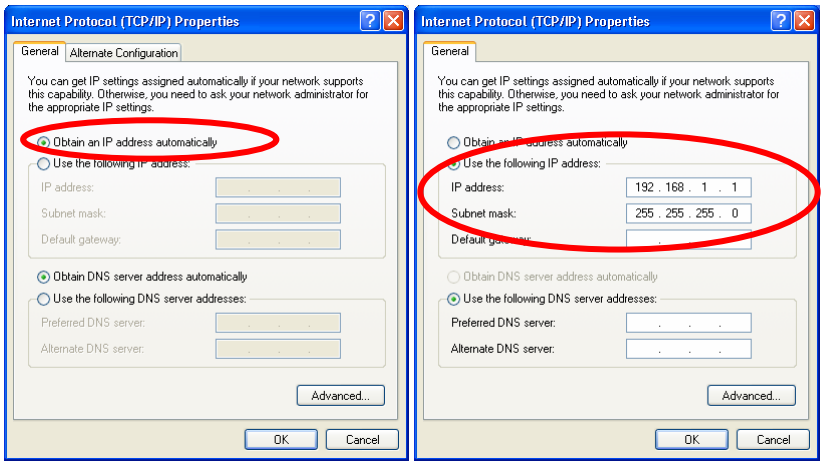
NETWORK CONNECTION

IP Address

***Note**: When assigning IP Addresses to the computers on the network, remember to have the IP address for each computer set on the same subnet mask. If your Broadband Router use DHCP technology, however, it won't be necessary for you to assign Static IP Address for your computer.*

1. To configure a dynamic IP address (i.e. if your broadband Router has the DHCP technology), check the **Obtain an IP Address Automatically** option.

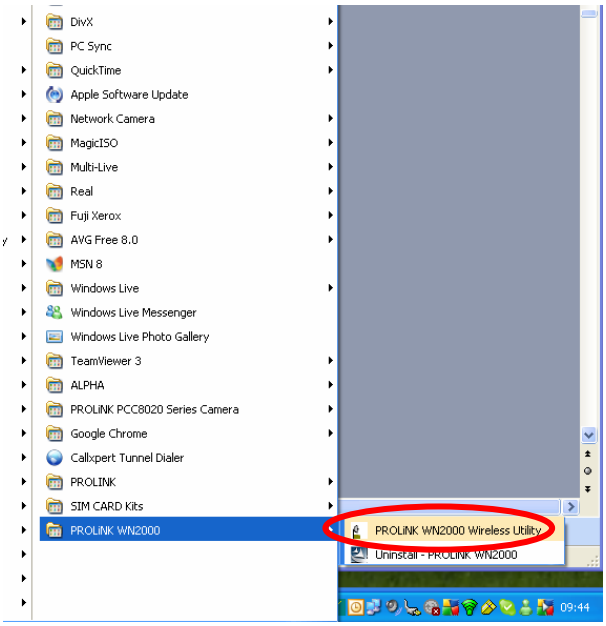
2. To configure a fixed IP address (if you broadband Router is not DHCP supported, or when you need to assign a static IP address), check the **Use the following IP address** option. Then, enter an IP address into the empty field; for example, enter ***192.168.1.1*** in the IP address field, and ***255.255.255.0*** for the Subnet Mask.


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel
Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Use the following IP address:
IP address:
192 . 168 . 1 . 1
Subnet mask:
255 . 255 . 255 . 0
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

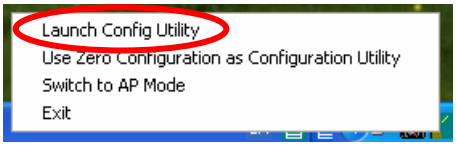
UTILITY CONFIGURATION FOR WINDOWS 2000/XP

After the Wireless adapter has been successfully installed, users can use the included Configuration Utility to set their preference.

Go to **Start→ (All) Program→ PROLiNK WN2000→ PROLiNK WN2000 Wireless Utility**.



You can also open the Configuration Utility by double clicking the icon or right clicking to select **Launch Config Utility**.



Station Mode

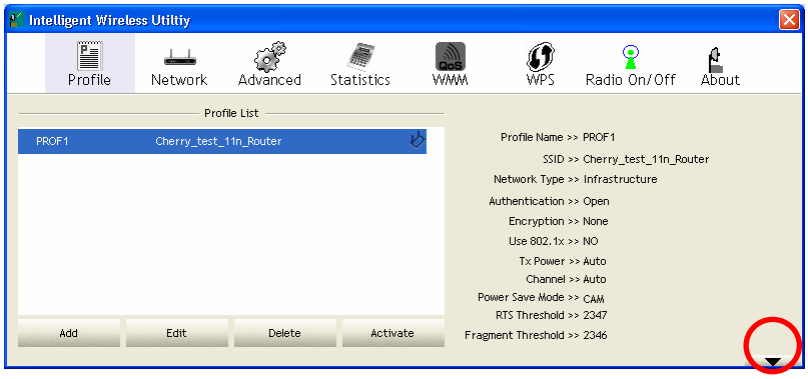
Notice: Under screen resolution 800 x 600 pixels, click the triangle button at the right down corner of the utility to expand the information of the station, the information will not be displayed completely.

Profile

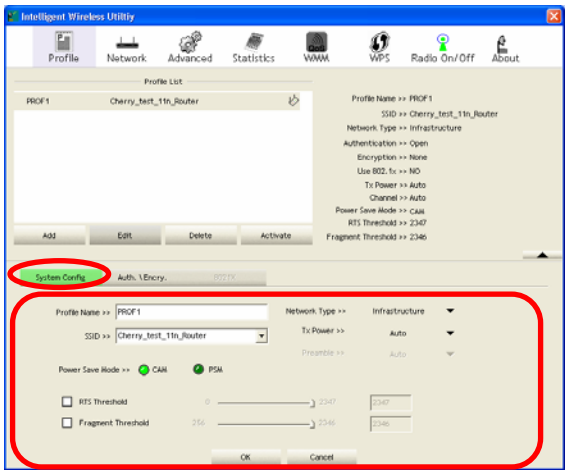
Profile can book keeping your favorite wireless setting among your home, office, and other public hot-spot. You may save multiple profiles, and activate the correct one at your preference. The Profile manager enables you to **Add, Edit, Delete** and **Activate** profiles.

Click this button to show the information of Status Section.

Click this button to hide the information of Status Section.



Profile Tab	
Profile Name	You can see a distinctive name of profile in this column. The default is PROF# (# 1, #2, #3....)
SSID	The **SSID** is the unique name shared among all points in your wireless network.

Network Type	Shows the network type of the device, including Infrastructure and Ad-Hoc.
Authentication	Shows the authentication mode.
Encryption	Shows the encryption type.
Use 802.1x	Whether or not use 802.1x feature.
Tx Power	Transmit power, the amount of power used by a radio transceiver to send the signal out.
Channel	Shows the selected channel that is currently in use.
Power Save Mode	Choose from CAM (Constantly Awake Mode) or PSM (Power Saving Mode.)
RTS Threshold	Shows the RTS Threshold of the device.
Fragment Threshold	Shows the Fragment Threshold of the device.
Add	Click to add a profile from the drop-down screen. **System Configuration tab:**  **Profile Name**: User can enter profile name, or use default name defined by system. The default is PROF# (# 1, #2, #3....).

SSID: The **SSID** is the unique name shared among all points in your wireless network. The name must be identical for all devices and points attempting to connect to the same network. User can use pull-down menu to select from available APs.

Power Save Mode:

- **CAM (Constantly Awake Mode)**: When this mode is selected, the power supply will be normally provided even when there is no throughput.
- **PSM (Power Saving Mode)**: When this mode is selected, this device will stay in power saving mode even when there is high volume of throughput.

Network Type: There are two types, **Infrastructure** and **Ad-hoc** modes. Under Ad-hoc mode user can also choose the preamble type, the available preamble type includes **Auto** and **Long**. In addition to that, the channel field will be available for setup in Ad-hoc mode.

- The **Infrastructure** is intended for the connection between wireless network cards and an Access Point. With the wireless adapter, you can connect wireless LAN to a wired global network via an Access Point.
- The **Ad-hoc** lets you set a small wireless workgroup easily and quickly. Equipped with the wireless adapter, you can share files and printers between each PC and laptop.

Tx Power: Transmit power, the amount of power used by a radio transceiver to send the signal out. Select the Tx power percentage from the pull-down list including **Auto, 100%, 75%, 50%, 25%, 10%** and **Lowest.**

Preamble: This function will show up when Ad-hoc network type be selected. A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. Select from the pull-down menu to change the

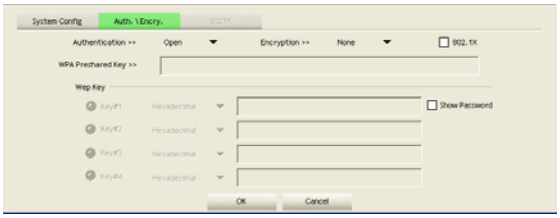
Preamble type into **Auto** or **Long**.

RTS Threshold: User can adjust the RTS threshold number by sliding the bar or key in the value directly. The default value is 2347. RTS/CTS Threshold is a mechanism implemented to prevent the "**Hidden Node**" problem. If the "Hidden Node" problem is an issue, users have to specify the packet size. *The RTS/CTS mechanism will be activated if the data size exceeds the value you set.*

This value should remain at its default setting of 2347. Should you encounter inconsistent data flow, only minor modifications of this value are recommended.

Fragment Threshold: User can adjust the Fragment threshold number by sliding the bar or key in the value directly. The default value is 2346. The mechanism of Fragmentation Threshold is used to improve the efficiency when high traffic flows along in the wireless network. If your Wireless LAN Adapter often transmits large files in wireless network, you can enter new Fragment Threshold value to split the packet. The value can be set from 256 to 2346.

Authentication and Security tab:



Authentication Type: There are several types of authentication modes including **Open, Shared, Leap, WPA, WPA-PSK, WPA2** and **WPA2-PSK**.

- **Open**: If your access point/wireless router is using "**Open"** authentication, then the wireless adapter will

need to be set to the same authentication type.

- **Shared**: Shared key is when both the sender and the recipient share a secret key.
- **LEAP:** Light Extensible Authentication Protocol. It is an EAP authentication type used primarily in Cisco Aironet WLANs. It encrypts data transmissions using dynamically generated WEP keys, and supports mutual authentication (only with CCX mode enabled.)
- **WPA/ WPA-PSK/ WPA2/ WPA2-PSK:** WPA or WPA-PSK authentications offer two encryption methods, TKIP and AES. For WPA-PSK, select the type of algorithm TKIP or AES and then enter a WPA Shared Key of 8-64 characters in the WPA Pre-shared Key field.

Encryption Type: For **Open** and **Shared** authentication mode, the selection of encryption type are **None** and **WEP**. For **WPA, WPA2, WPA-PSK** and WP**A2-PSK** authentication mode, the encryption type supports both **TKIP** and **AES**.

WPA Pre-shared Key: This is the shared secret between AP and STA. For WPA-PSK and WPA2-PSK authentication mode, this field must be filled with character longer than 8 and less than 64 lengths.

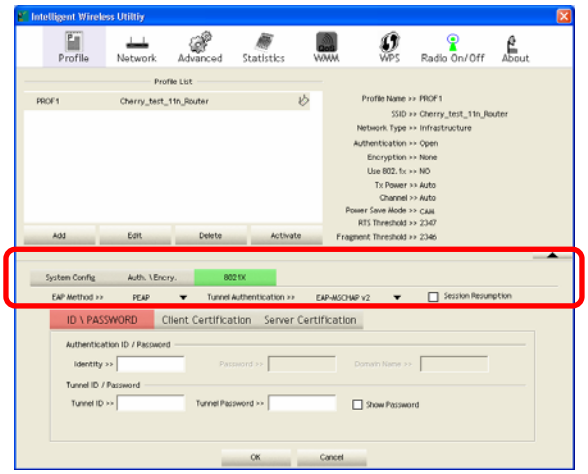
WEP Key: Only valid when using WEP encryption algorithm. The key must match with the AP's key. There are several formats to enter the keys.

- Hexadecimal (128bits): 26 Hex characters (0~9, a~f).
- ASCII (128bits): 13 ASCII characters.

Show Password: Check this box to show the password you en02tered.

802.1x Setting: When user use radius server to authenticate client certificate for WPA authentication mode (WPA authentication do not support EAP Method-MD5-Challenge).

802.1x tab:



EAP Method:

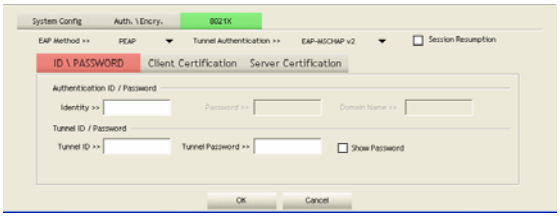
- **PEAP**: Protect Extensible Authentication Protocol. PEAP transport securely authentication data by using tunnelling between PEAP clients and an authentication server. PEAP can authenticate wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure wireless LAN.
- **TLS / Smart Card**: Transport Layer Security. Provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform

	authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point. • **TTLS**: Tunnelled Transport Layer Security. This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates. • **EAP-FAST**: Flexible Authentication via Secure Tunnelling. It was developed by Cisco. Instead of using a certificate, mutual authentication is achieved by means of a PAC (Protected Access Credential) which can be managed dynamically by the authentication server. The PAC can be provisioned (distributed one time) to the client either manually or automatically. Manual provisioning is delivery to the client via disk or a secured network distribution method. Automatic provisioning is an in-band, over the air, distribution. For tunnel authentication, only support "Generic Token Card" authentication now. • **MD5-Challenge**: Message Digest Challenge. Challenge is an EAP authentication type that provides base-level EAP support. It provides for only one-way authentication - there is no mutual authentication of wireless client and the network. (Only Open and Shared authentication mode can use this function.) **Tunnel Authentication**: • **Protocol**: Tunnel protocol, List information including **EAP-MSCHAP v2**, **EAP-TLS/ Smart Card**, and **Generic Token Card**. • **Tunnel Identity**: Identity for tunnel.

- **Tunnel Password**: Password for tunnel.

Session Resumption: Reconnect the signal while broken up, to reduce the packet and improve the transmitting speed. User can click the box to enable or disable this function.

ID\PASSWORD tab:

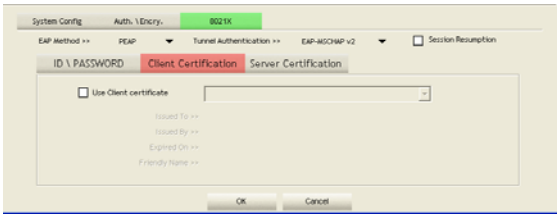


ID/ PASSWORD: Identity and password for server.

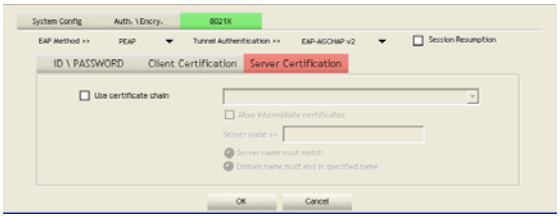
- **Authentication ID / Password**: Identity, password and domain name for server. Only "EAP-FAST" EAP method and "LEAP" authentication can key in domain name. Domain name can be keyed in blank space.
- **Tunnel ID / Password:** Identity and Password for server.

Show Password: Check this box to show the password you entered.
OK: Click to save settings and exit this page.
Cancel: Click to call off the settings and exit.

Client Certification tab:

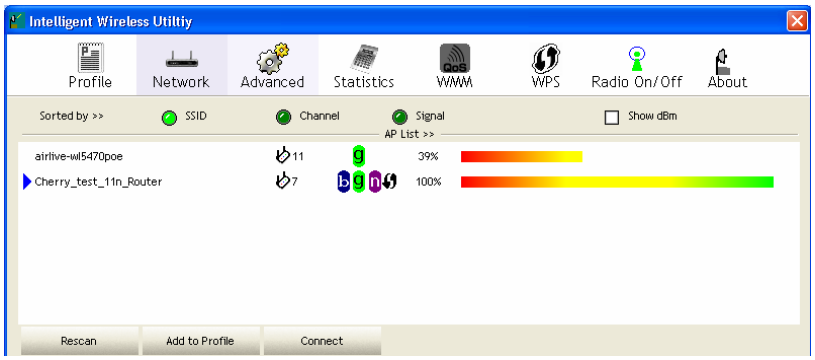


Use Client certificate: Choose to enable server

	authentication. **OK**: Click to save settings and exit this page. **Cancel:** Click to call off the settings and exit. **Server Certification tab:**  **Use certificate chain**: Choose use server that issuer of certificates. **Allow intimidate certificates**: It must be in the server certificate chain between the server certificate and the server specified in the certificate issuer must be field. **Server name**: Enter an authentication sever root. **Server name must match:** Click to enable or disable this function. **Domain name must end in specified name:** Click to enable or disable this function. **OK**: Click to save settings and exit this page. **Cancel:** Click call off the settings and exit.
Delete	Click to delete an existing profile.
Edit	Click to edit a profile.
Activate	Click to make a connection between devices.

Network

The Network page displays the information of surrounding APs from last scan result. The tab lists the information including SSID, Network type, Channel, Wireless mode, Security-Enabled and Signal.

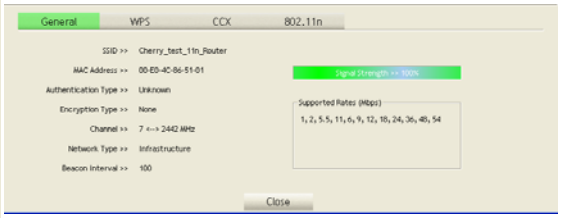
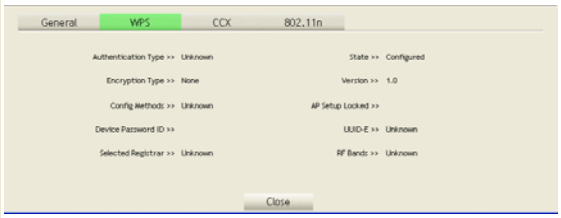


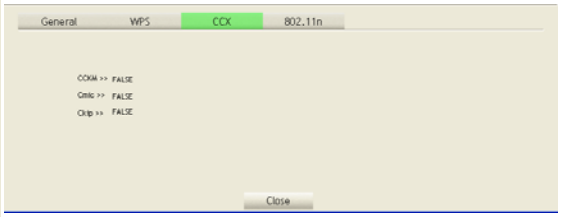
Network Tab	
Sorted by	Indicate that AP list are sorted by SSID, Channel or Signal.
Show dBm	Check the box to show the dBm of the AP list.
SSID	Shows the name of BSS network.
Network Type	Network type in use, Infrastructure for BSS, Ad-Hoc for IBSS network.
Channel	Shows the currently used channel.
Wireless mode	AP support wireless mode. It may support 802.11b, 802.11g or 802.11n wireless mode.
Encryption	Shows the encryption type currently in use. Valid value includes WEP, TKIP, AES, Not Use and WPS.
Signal	Shows the receiving signal strength of specified network.
Rescan	Click to refresh the AP list.
Add to Profile	Select an item on the list and then click to add it into the profile list.

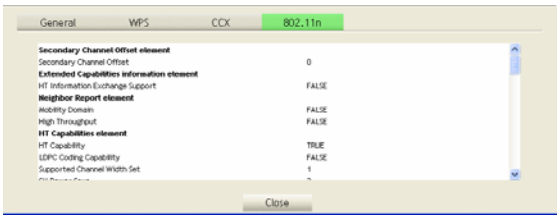
Connect	Select an item on the list and then click to make a connection.

AP Information

When you double click on the intended AP, you can see AP's detail information that divides into four parts. They are General, WPS, CCX and 802.11n information. The introduction is as following:

General	 General information contain AP's SSID, MAC address, Authentication Type, Encryption Type, Channel, Network Type, Beacon Interval, Signal Strength and Supported Rates. **Close**: Click this button to exit the information screen.
WPS	 WPS information contains Authentication Type, Encryption Type, Config Methods, Device Password ID, Selected Registrar, State, Version, AP Setup Locked, UUID-E and RF Bands.

	Authentication Type: There are four types of authentication modes supported by RaConfig. They are Open, Shared, WPA-PSK and WPA system. **Encryption Type**: For Open and Shared authentication mode, the selection of encryption type are None and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES. **Config Methods**: Correspond to the methods the AP supports as an Enrollee for adding external Registrars. **Device Password ID**: Indicate the method or identifies the specific password that the selected Registrar intends to use. **Selected Registrar**: Indicate if the user has recently activated a Registrar to add an Enrollee. The values are "TRUE" and "FALSE". **State**: The current configuration state on AP. The values are "Unconfigured" and "Configured". **Version**: WPS specified version. **AP Setup Locked**: Indicate if AP has entered a setup locked state. **UUID-E**: The universally unique identifier (UUID) element generated by the Enrollee. There is a value. It is 16 bytes. **RF Bands**: Indicate all RF bands available on the AP. A dual-band AP must provide it. The values are "2.4GHz". **Close**: Click this button to exit the information screen.
CXX	

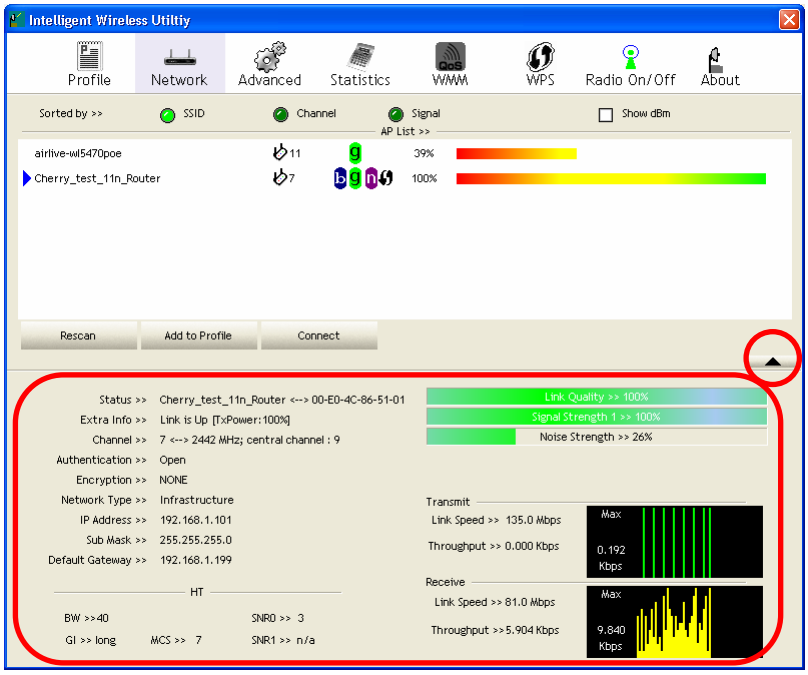
	CCX information contains CCKM, Cmic and Ckip information. **Close**: Click this button to exit the information screen.
802.11n	 This tab will show up if you select the AP that support 11n mode. Here shows the connected AP 802.11n related information.

Link Status

Click the triangle button at the right down corner of the windows to expand the link status. The link status page displays the detail information of current connection.

Click this button to show the information of Status Section.

Click this button to hide the information of Status Section.

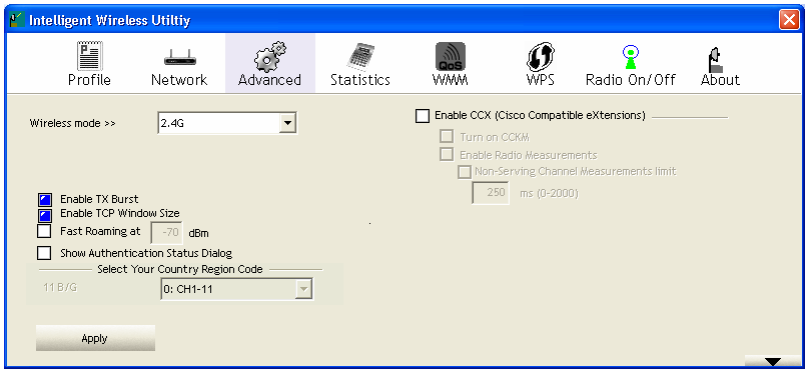


Link Status Tab	
Status	Shows the current connected AP SSID and MAC address. If there is no connection existing, it will show Disconnected.
Extra Info	Shows the link status and Tx power percentage.
Channel	Shows the current channel in use.
Authentication	Authentication mode used within the network, including Unknown, WPA-PSK, WPA2-PSK, WPA and WPA2.
Encryption	Shows the encryption type currently in use. Valid value includes WEP, TKIP, AES, and Not Use.

Network Type	Network type in use, Infrastructure for BSS, Ad-Hoc for IBSS network.
IP Address	Shows the IP address information.
Sub Mask	Shows the Subnet Mask information.
Default Gateway	Shows the default gateway information.
Link Quality	Shows the connection quality based on signal strength and TX/RX packet error rate.
Signal Strength 1	Shows the Receiving signal strength, you can choose to display as percentage or dBm format.
Noise Strength	Shows the noise signal strength in the wireless environment.
Transmit	Shows the current Link Speed and Throughput of the transmit rate.
Receive	Shows the current Link Speed and Throughput of receive rate.
Link Speed	Shows the current transmitting rate and receiving rate.
Throughput	Shows the transmitting and receiving speed of data.

Advanced

This Advanced page provides advanced and detailed settings for your wireless network.

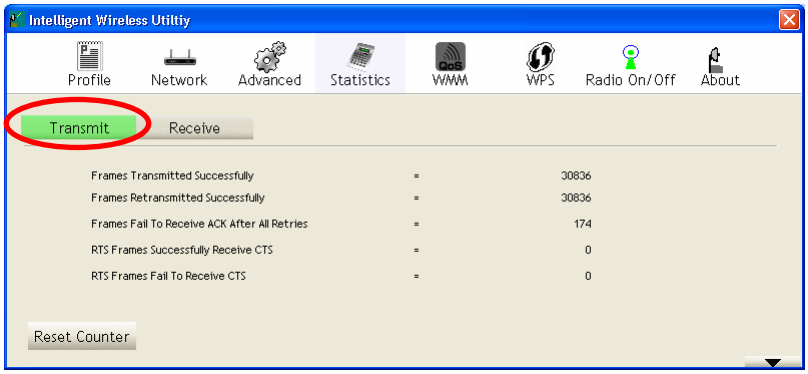


Advanced Tab	
Wireless mode	Here supports 2.4G (included 802.11b/g/n) wireless mode.
Enable TX Burst	Check to enable this function. This function enables the adapter to deliver better throughput during a period of time, it only takes effect when connecting with the AP that supports this function.
Enable TCP Window Size	Check to increase the transmission quality. The large TCP window size the better performance.
Fast Roaming at dBm	Check to set the roaming interval, fast to roaming, setup by transmits power. Default setting is -70dBm.
Show Authentication Status Dialog	When you connect AP with authentication, choose whether show "Authentication Status Dialog" or not. Authentication Status Dialog displays the process about 802.1x authentications.
Enable CCX (Cisco Compatible extensions)	Check to enable the CCX function. • Turn on CCKM. • Enable Radio Measurements: Check to enable the Radio measurement function. • Non-Serving Measurements limit: User can set channel measurement every 0~2000 milliseconds. Default is set to 250 milliseconds.

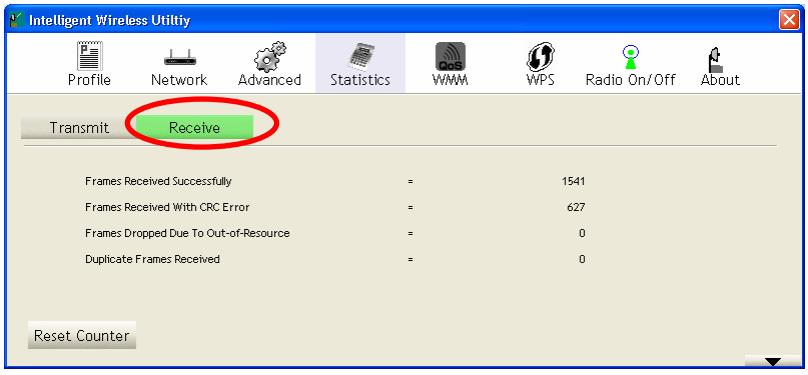
Apply	Click to apply above settings.

Statistics

The Statistics screen displays the statistics on your current network settings.



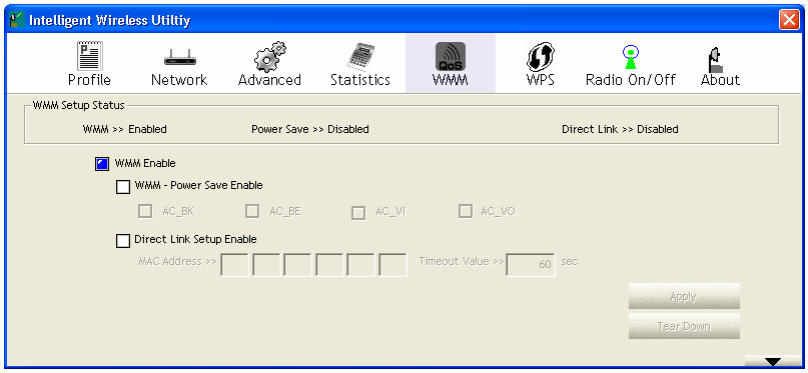
Transmit	
Frames Transmitted Successfully	Shows information of frames successfully sent.
Frames Retransmitted Successfully	Shows information of frames successfully sent with one or more reties.
Frames Fail To Receive ACK After All Retries	Shows information of frames failed transmit after hitting retry limit.
RTS Frames Successfully Receive CTS	Shows information of successfully receive CTS after sending RTS frame
RTS Frames Fail To Receive CTS	Shows information of failed to receive CTS after sending RTS.
Reset Counter	Click this button to reset counters to zero.



Receive Statistics	
Frames Received Successfully	Shows information of frames Received Successfully.
Frames Received With CRC Error	Shows information of frames received with CRC error.
Frames Dropped Due To Out-of-Resource	Shows information of frames dropped due to resource issue.
Duplicate Frames Received	Shows information of frames received more than twice.
Reset Counter	Click this button to reset counters to zero.

WMM / QoS

The WMM page shows the Wi-Fi Multi-Media power save function and Direct Link Setup that ensure your wireless network quality.

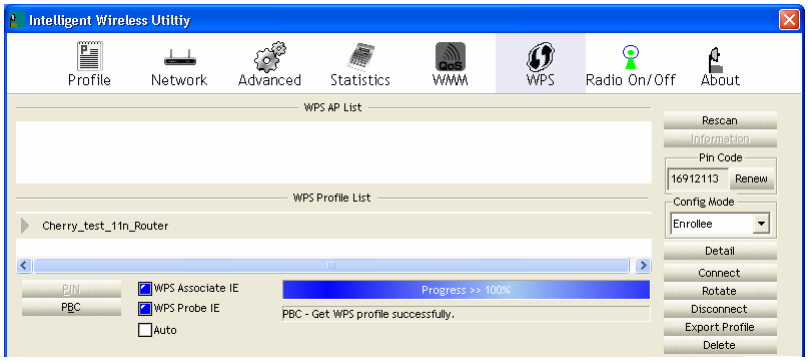


WMM Enable	Check the box to enable Wi-Fi Multi-Media function that is meant to improve audio, video and voice applications transmitted over Wi-Fi.
WMM- Power Save Enable	Select which ACs you want to enable the power saving mode. AC_BK (Access Category Background) AC_BE (Access Category Best Effort) AC_VI (Access Category Video) AC_VO (Access Category Voice)
Direct Link Setup Enable	Check the box to enable Direct Link Setup.
MAC Address	The setting of DLS(Direct Link Setup) indicates as follow : Fill in the blanks of Direct Link with MAC Address of STA, and the STA must conform to two conditions: • Connecting with the same AP that supports DLS feature. • DLS enabled.
Timeout Value	Timeout Value represents that it disconnect automatically after few seconds. The value is integer that must be between 0~65535. It represents that it always connects if the value is zero. Default value of Timeout Value is 60 seconds.

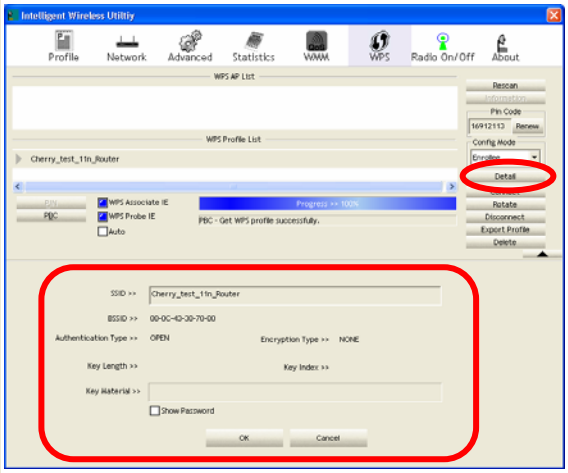
Apply	Click this button to apply the settings.
Tear Down	Select a direct link STA, then click "Tear Down" button to disconnect the STA.

WPS

The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simplify the security setup and management of Wi-Fi networks. The STA as an Enrollee or external Registrar supports the configuration setup using PIN (Personal Identification Number) configuration method or PBC (Push Button Configuration) method through an internal or external Registrar.



WPS AP List	Display the information of surrounding APs with WPS IE from last scan result. List information included SSID, BSSID, Channel, ID (Device Password ID), Security-Enabled.
Rescan	Issue a rescan command to wireless NIC to update information on surrounding wireless network.
Information	Display the information about WPS IE on the selected

	network. List information included Authentication Type, Encryption Type, Config Methods, Device Password ID, Selected Registrar, State, Version, AP Setup Locked, UUID-E and RF Bands.
PIN Code	8-digit numbers. It is required to enter PIN Code into Registrar when using PIN method. When STA is Enrollee, you can use "Renew" button to re-generate new PIN Code.
Config Mode	Select from the pull-down menu to decide the station role-playing as an Enrollee or an external Registrar.
Detail	Click the Detail button to show the information about Security and Key in the credential.  If you select the AP that listed in the WPS Profile List field, you can click the **Detail** button to see more AP information. **SSID**: Shows the connected AP network name.

	BSSID: The MAC address of the connected AP. Fixed and cannot be changed. **Authentication Type**: The authentication type support Open, WPA-PSK and WPA2-PSK. **Encryption Type:** For **Open** authentication mode, the selection of encryption type are **NONE** and **WEP**. For **WPA-PSK** and **WPA2-PSK** authentication mode, the encryption type supports both **TKIP** and **AES**. **Key Length:** Only valid when using **Open** authentication mode and **WEP** encryption. There are key lengths 5, 10, 13 and 26. **Key Index:** Only valid when using **Open** authentication mode and **WEP** encryption. There are 1~4 key index. **Key Material:** The key material can be used to ensure the security of your wireless network. Fill in the appropriate value or phrase in **Key Material** field. **Show Password**: Check this box to show the passwords that have been entered. **OK**: Click to save and apply the new settings. **Cancel**: Click to leave and discard the settings.
Connect	Command to connect to the selected network inside credentials. The active selected credential is as like as the active selected Profile.
Rotate	Command to rotate to connect to the next network inside credentials.
Disconnect	Stop WPS action and disconnect this active link. And then select the last profile at the Profile Page. If there is an empty profile page, the driver will select any non-security AP.
Export Profile	Export all credentials to Profile.

Delete	Delete an existing credential. And then select the next credential if exist. If there is an empty credential, the driver will select any non-security AP.
PIN	Start to add to Registrar using PIN (Personal Identification Number) configuration method. If STA Registrar, remember that enter PIN Code read from your Enrollee before starting PIN.
PBC	Start to add to AP using PBC (Push Button Configuration) method.
WPS Associate IE	Send the association request with WPS IE during WPS setup. It is optional for STA.
WPS Probe IE	Send the probe request with WPS IE during WPS setup. It is optional for STA.
Auto	Check this box the device will connect the AP automatically.
Progress Bar	Display rate of progress from Start to Connected status.
Status Bar	Display currently WPS Status.

Radio On/Off

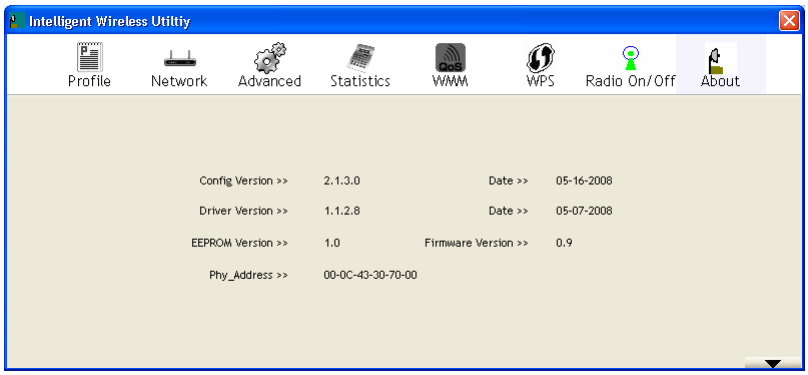
Click this Radio On/Off button to turn ON or OFF radio function.

This icon shows radio on, click to turn it off.

This icon shows radio off, click to turn it on.

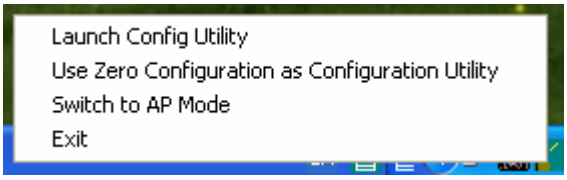
About

This page displays the information of the wireless card including, Config Version/ Date, Driver Version/ Date, EEPROM Version, Firmware Version and Phy_Address.



Utility Menu List

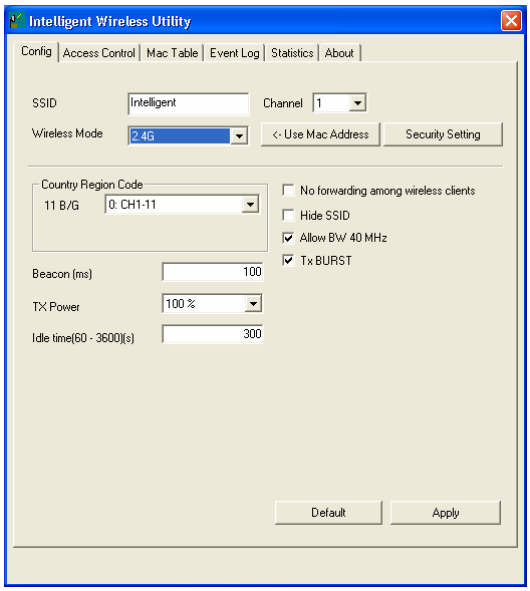
To access the utility menu list, please right click the utility icon on the task bar.



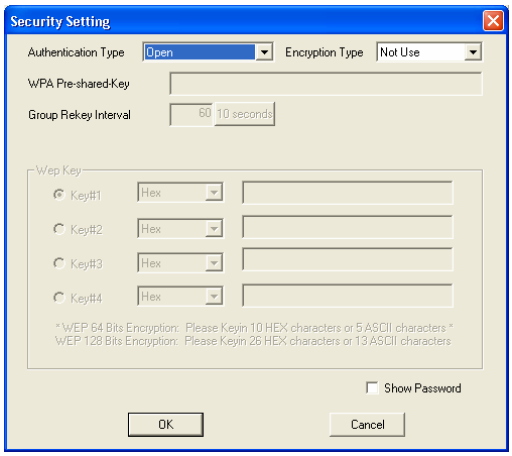
- **Launch Config Utility**: Select to open the utility screen.
- **Use Zero Configuration as Configuration Utility**: Select to use the Window XP built-in utility (Zero configuration utility).
- **Switch to AP Mode**: Select to make your wireless USB adapter act as a wireless AP.
- **Exit**: Select to close the utility program.

Soft AP mode

Config



Config	
SSID	AP name of user type. User also can click **Use Mac Address** button to display it.
Channel	Manually force the AP using the channel. The system default is CH 1.
Wireless mode	Here supports 2.4G (included 802.11b/g/n) wireless mode.
Use Mac Address	Click this button to replace SSID by MAC address.
Security Setting	Authentication mode and encryption algorithm used within the AP. The system default is no authentication and encryption.



Authentication Type: There are several types of authentication modes including Open, Shared, WPA-PSK, WPA2-PSK, and WPA-PSK/ WPA2-PSK.

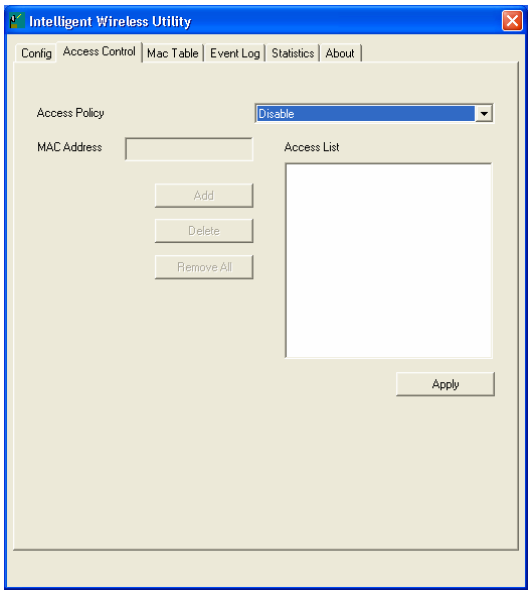
Encryption Type: For **Open** and **Shared** authentication mode, the selections of encryption type are **Not Use** and **WEP**. For **WPA-PSK**, **WPA2-PSK**, and **WPA-PSK/ WPA2-PSK** authentication mode, the encryption type supports both **TKIP** and **AES**.

WPA Pre-shared Key: This is the shared secret between AP and STA. For WPA-PSK and WPA2-PSK and WPA-PSK/ WPA2-PSK authentication mode, this field must be filled with character longer than 8 and less than 64 lengths.

Group Re-key Interval: Only valid when using WPA-PSK, WPA2-PSK, and WPA-PSK/ WPA2-PSK authentication mode to renew key. User can set to change by seconds or packets. Default is 600 seconds.

	WEP Key: Only valid when using WEP encryption algorithm. The key must match with the AP's key. There are two formats to enter the keys. • Hexadecimal (128bits): 26 Hex characters. • ASCII (128bits): 13 ASCII characters. **Show Password**: Check this box to show the password you entered.
Beacon (ms)	The time between two beacons. The system default is 100 ms.
TX Power	Manually force the AP transmits power from the pull down list 100%, 75%, 50%, 25% and lowest. The system default is 100%.
Idle time(60-3600)(s)	It represents that the AP will idle after few seconds. The time must be set between 60~3600 seconds. Default value of idle time is 300 seconds.
No forwarding among wireless clients	No beacon among wireless client, clients can share information each other. The system default is no forwarding.
Hide SSID	Do not display AP name. System default no hide.
Allow BW 40MHz	Click to disable this function. Default is enabled.
Tx BURST	Check to enable this function.
Default	Use the system default value.
Apply	Click to apply the above settings.

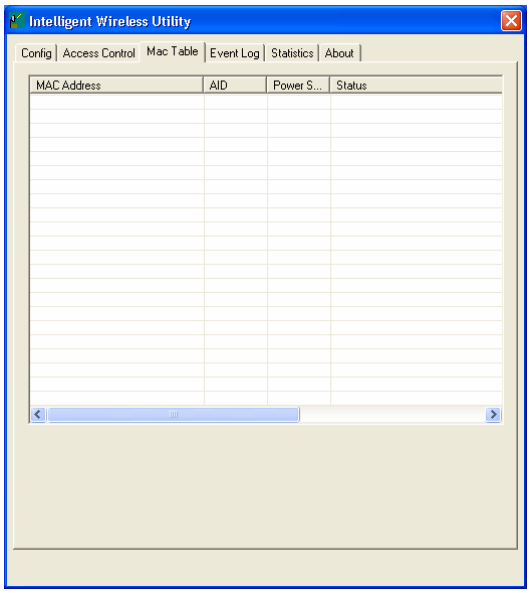
Access Control



Access Control	
Access Policy	User chooses whether AP start the function or not. System default is Disable. ● **Disable:** Do not use this access control function. ● **Allow All:** Only the MAC address listed in the Access List can connect with this soft AP. ● **Reject All:** Only the MAC address listed in the Access List can NOT connect with this soft AP.
Mac Address	Manually force the Mac address using the function. Click Add and the MAC address will be listed in the Access List pool.
Access List	Display all Mac Address that you have set.

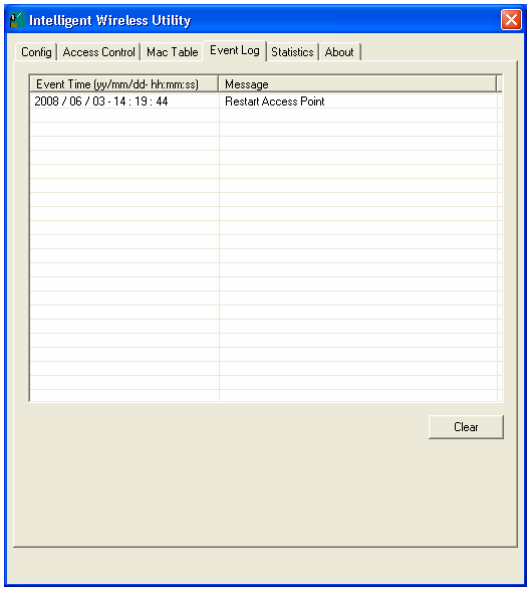
Add	Add the MAC address that you would like to set.
Delete	Delete the Mac address that you have set.
Remove All	Remove all Mac address in the Access List.
Apply	Apply the above changes.

MAC Table



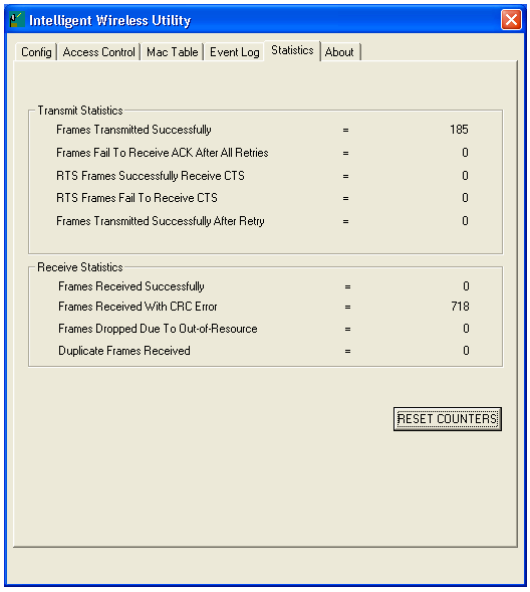
MAC Table	
MAC Address	The station MAC address of current connection.
AID	Raise value by current connection.
Power Saving Mode	The station of current connect whether it have to support.
Status	The status of current connection.

Event Log



Event Log	
Event Time (yy/mm/dd-hh:mm:ss)	Records the event time.
Message	Records all the event messages.

Statistics

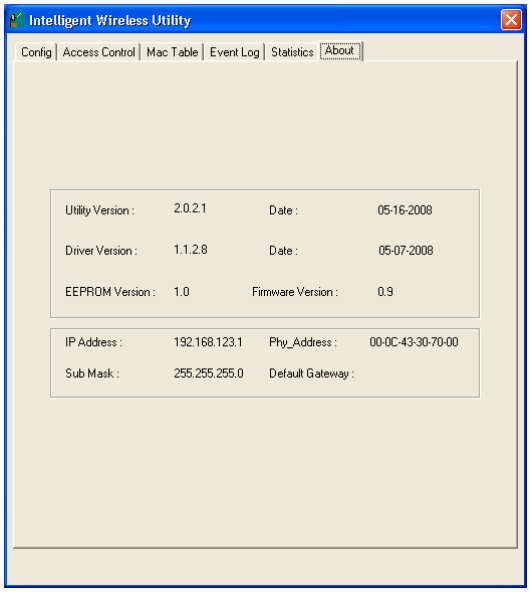

Intelligent Wireless Utility
Config
Access Control
Mac Table
Event Log
Statistics
About
Transmit Statistics
Frames Transmitted Successfully = 185
Frames Fail To Receive ACK After All Retries = 0
RTS Frames Successfully Receive CTS = 0
RTS Frames Fail To Receive CTS = 0
Frames Transmitted Successfully After Retry = 0
Receive Statistics
Frames Received Successfully = 0
Frames Received With CRC Error = 718
Frames Dropped Due To Out-of-Resource = 0
Duplicate Frames Received = 0
RESET COUNTERS

Transmit Statistics	
Frames Transmitted Successfully	Frames successfully sent.
Frames Fail To Receive ACK After All Retries	Frames failed transmit after hitting retry limit.
RTS Frames Successfully Receive CTS	Successfully receive CTS after sending RTS frame
RTS Frames Fail To Receive CTS	Failed to receive CTS after sending RTS.
Frames Transmitted Successfully After Retry	Frames successfully sent with one or more reties.

Receive Statistics	
Frames Received Successfully	Frames Received Successfully
Frames Received With CRC Error	Frames received with CRC error.
Frames Dropped Due To Out-of-Resource	Frames dropped due to resource issue
Duplicate Frames Received	Duplicate received frames.
Reset Counter	Reset counters to zero.

About

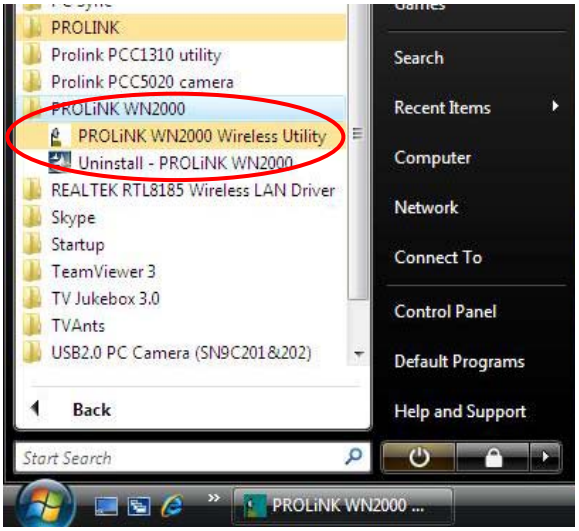
This page displays the wireless card and driver version information.



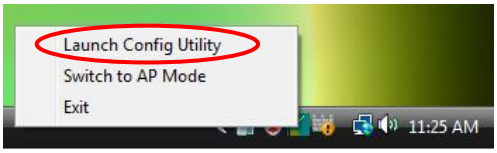
UTILITY CONFIGURATION FOR WINDOWS VISTA

After the Wireless adapter has been successfully installed, users can use the included Configuration Utility to set their preference.

Go to **Start→ (All) Program→ PROLiNK WN2000 → ROLiNK WN2000 Wireless Utility**.



You can also open the Configuration Utility by double clicking the icon or right clicking to select **Launch Config Utility**.



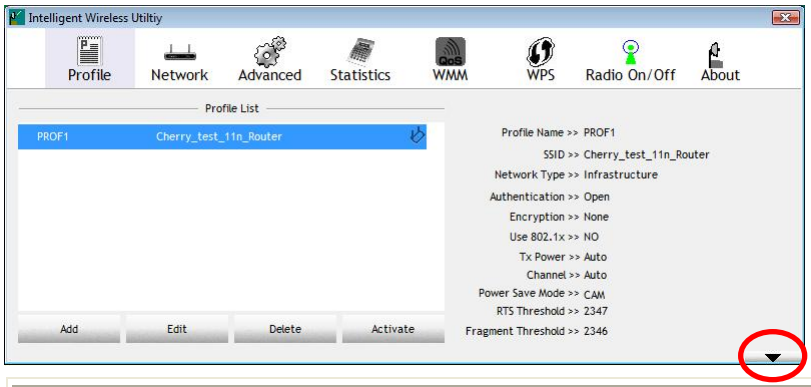
Station Mode

Profile

Profile can book keeping your favorite wireless setting among your home, office, and other public hot-spot. You may save multiple profiles, and activate the correct one at your preference. The Profile manager enables you to **Add, Edit, Delete** and **Activate** profiles.

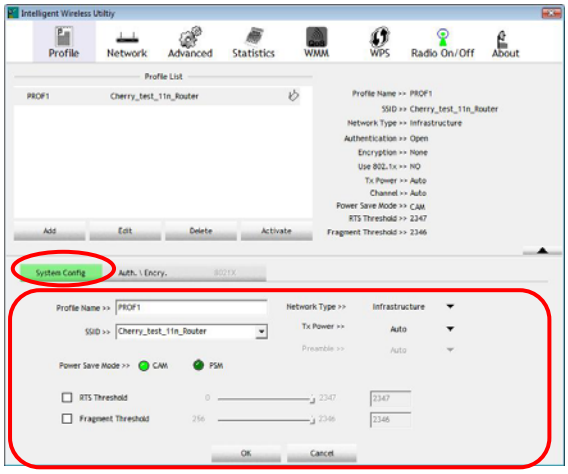
Click this button to show the information of Status Section.

Click this button to hide the information of Status Section.



Profile Tab	
Profile Name	You may enter a distinctive name of profile in this column. The default is PROF# (# 1, #2, #3....)
SSID	The **SSID** is the unique name shared among all points in your wireless network.
Network Type	Shows the network type of the device, including Infrastructure and Ad-Hoc.

Authentication	Shows the authentication mode.
Encryption	Shows the encryption type.
Use 802.1x	Whether use 802.1x feature or not.
Tx Power	Transmit power, the amount of power used by a radio transceiver to send the signal out.
Channel	Shows the selected channel that is currently in use.
Power Save Mode	Choose from CAM (Constantly Awake Mode) or PSM (Power Saving Mode.)
RTS Threshold	Shows the RTS Threshold of the device.
Fragment Threshold	Shows the Fragment Threshold of the device.
Add	Click to add a profile from the drop-down screen. **System Configuration tab:**



Profile Name: User can enter profile name, or use default name defined by system. The default is PROF# (# 1, #2, #3....).

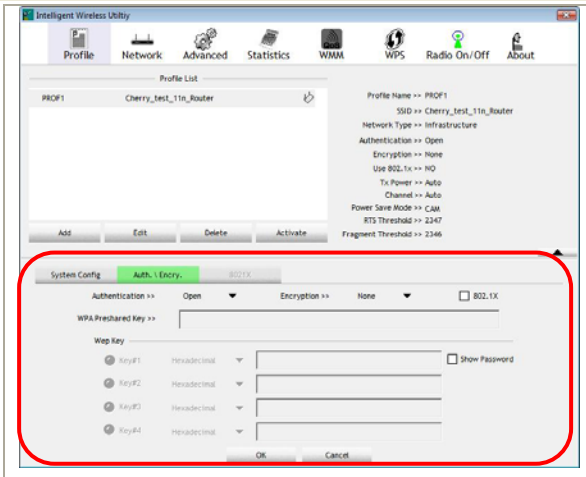
SSID: The **SSID** is the unique name shared among all points in your wireless network. The name must be identical for all devices and points attempting to connect to the same network. User can use pull-down menu to select from available APs.

Network Type: There are two types, Infrastructure and Ad hoc modes.

- The **Infrastructure** is intended for the connection between wireless network cards and an Access Point. With the wireless adapter, you can connect wireless LAN to a wired global network via an Access Point.

- The **Ad hoc** lets you set a small wireless workgroup easily and quickly. Equipped with the wireless adapter, you can share files and printers between each PC and laptop.

	Tx Power: Transmit power, the amount of power used by a radio transceiver to send the signal out. Select the Tx power percentage from the pull-down list including **Auto, 100%, 75%, 50%, 25%, 10%** and **Lowest.** **Preamble**: This function will show up when Ad-hoc network type be selected. A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. Select from the pull-down menu to change the Preamble type into **Auto** or **Long**. **RTS Threshold**: User can adjust the RTS threshold number by sliding the bar or key in the value directly. The default value is 2347. RTS/CTS Threshold is a mechanism implemented to prevent the "**Hidden Node**" problem. If the "Hidden Node" problem is an issue, users have to specify the packet size. *The RTS/CTS mechanism will be activated if the data size exceeds the value you set.* This value should remain at its default setting of 2347. Should you encounter inconsistent data flow, only minor modifications of this value are recommended. **Fragment Threshold**: User can adjust the Fragment threshold number by sliding the bar or key in the value directly. The default value is 2346. The mechanism of Fragmentation Threshold is used to improve the efficiency when high traffic flows along in the wireless network. If your Wireless LAN Adapter often transmits large files in wireless network, you can enter new Fragment Threshold value to split the packet. The value can be set from 256 to 2346. **Authentication and Encryption tab:**



Authentication Type: There are six type of authentication modes including Open, Shared, WPA, WPA-PSK, WPA2 and WPA2-PSK.

- **Open**: If your access point/ wireless router is using "**Open"** authentication, then the wireless adapter will need to be set to the same authentication type.
- **Shared**: Shared key is when both the sender and the recipient share a secret key.
- **WPA/ WPA-PSK/ WPA2/ WPA2-PSK:** WPA-PSK offers two encryption methods, TKIP and AES. Select the type of algorithm, TKIP or AES and then enter a WPA Shared Key of 8-63 characters in the WPA Pre-shared Key field.

Encryption Type: For **Open** and **Shared** authentication mode, the selection of encryption type are **None** and **WEP**. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES.

WPA Pre-shared Key: This blank is the shared secret between AP and STA. For WPA-PSK and WPA2-PSK authentication mode, this field must be filled with character longer than 8 and less than 64 lengths.

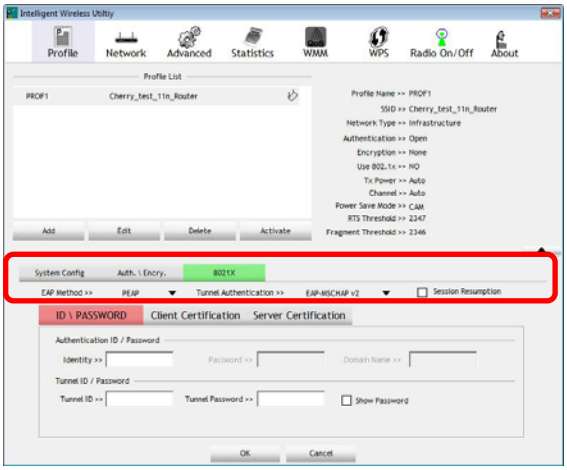
WEP Key: Only valid when using WEP encryption algorithm. The key must match with the AP's key. There are several formats to enter the keys.

- Hexadecimal (128bits): 26 Hex characters (0~9, a~f).
- ASCII (128bits): 13 ASCII characters.

Show Password: Check this box to show the password you entered.

802.1x Setting: When user use radius server to authenticate client certificate for WPA authentication mode.

802.1x tab:



EAP Method:

	• **PEAP**: Protect Extensible Authentication Protocol. PEAP transport securely authentication data by using tunnelling between PEAP clients and an authentication server. PEAP can authenticate wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure wireless LAN. • **TLS** / **Smart Card**: Transport Layer Security. Provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point. **Tunnel Authentication**: • **Protocol**: Tunnel protocol, List information including **EAP-MSCHAP v2** and **EAP-TLS/ Smart Card.** • **Tunnel Identity**: Identity for tunnel. • **Tunnel Password**: Password for tunnel. **Session Resumption**: Reconnect the signal while broken up, to reduce the packet and improve the transmitting speed. User can click the box to enable or disable this function. **ID\PASSWORD tab:**

ID/ PASSWORD: Identity and password for server.

- **Authentication ID / Password**: Identity, password and domain name for server. Only "EAP-FAST" and "LEAP" authentication can key in domain name. Domain name can be keyed in blank space.

- **Tunnel ID / Password:** Identity and Password for server.

Show Password: Check this box to show the password you entered.

OK: Click to save settings and exit this page.

Cancel: Click to call off the settings and exit.

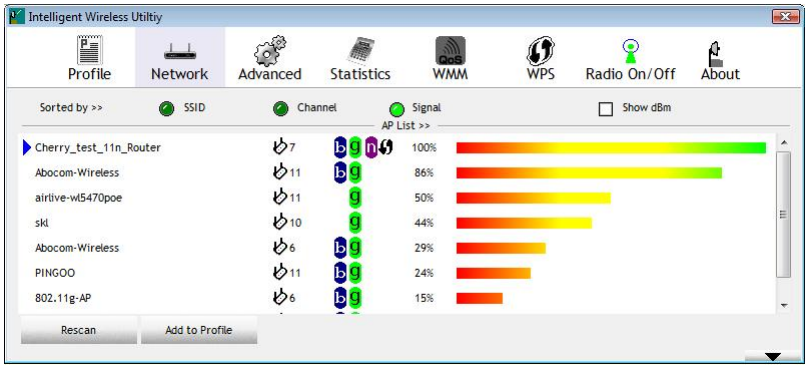
Client Certification tab:

You can select **Use a certificate on this computer**, a client certificate for server authentication. Or you can select **Use my smart card** to enable the Client

	Certification function. **OK**: Click to save settings and exit this page. **Cancel:** Click to call off the settings and exit. **Server Certification tab:** **Use certificate chain**: Choose use server that issuer of certificates. **Server name**: Enter an authentication sever name. **OK**: Click to save settings and exit this page. **Cancel:** Click call off the settings and exit.
Delete	Click to delete an existing profile.
Edit	Click to edit a profile.
Activate	Click to make a connection between devices.

Network

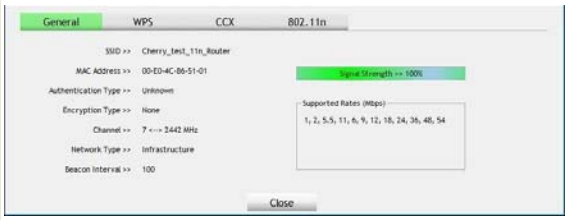
The Network page displays the information of surrounding APs from last scan result. The tab lists the information including SSID, Network type, Channel, Wireless mode, Security-Enabled and Signal.



Network Tab	
Sorted by	Indicate that AP list are sorted by SSID, Channel or Signal.
Show dBm	Check the box to show the dBm of the AP list.
SSID	Shows the name of BSS network.
Network Type	Network type in use, Infrastructure for BSS, Ad-Hoc for IBSS network.
Channel	Shows the currently used channel.
Wireless mode	AP support wireless mode. It may support 802.11b or 802.11g or 802.11n wireless mode.
Encryption	Shows the encryption type currently in use. Valid value includes WEP, TKIP, AES, and Not Use.
Signal	Shows the receiving signal strength of specified network.
Rescan	Click to refresh the AP list.
Add to Profile	Select an item on the list and then click to add it into the profile list.

AP information

When you double click on the intended AP, you can see AP's detail information that divides into three parts. They are General, WPS, CCX information. The introduction is as following:

General	 General information contain AP's SSID, MAC address, Authentication Type, Encryption Type, Channel, Network Type, Beacon Interval, Signal Strength and Supported Rates. **Close**: Click this button to exit the information screen.
WPS	 WPS information contains Authentication Type, Encryption Type, Config Methods, Device Password ID, Selected Registrar, State, Version, AP Setup Locked, UUID-E and RF Bands. **Authentication Type**: There are four types of authentication modes supported by RaConfig. They are Open, Shared, WPA-PSK and WPA system. **Encryption Type**: For open and shared authentication mode, the selection of encryption type are None and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES. **Config Methods**: Correspond to the methods the AP supports as an Enrollee for adding external Registrars.

	Device Password ID: Indicate the method or identifies the specific password that the selected Registrar intends to use. **Selected Registrar**: Indicate if the user has recently activated a Registrar to add an Enrollee. The values are "TRUE" and "FALSE". **State**: The current configuration state on AP. The values are "Unconfigured" and "Configured". **Version**: WPS specified version. **AP Setup Locked**: Indicate if AP has entered a setup locked state. **UUID-E**: The universally unique identifier (UUID) element generated by the Enrollee. There is a value. It is 16 bytes. **RF Bands**: Indicate all RF bands available on the AP. A dual-band AP must provide it. The values are "2.4GHz". **Close**: Click this button to exit the information screen.
CXX	 CCX information contains CCKM, Cmic and Ckip information. **Close**: Click this button to exit the information screen.
802.11n	

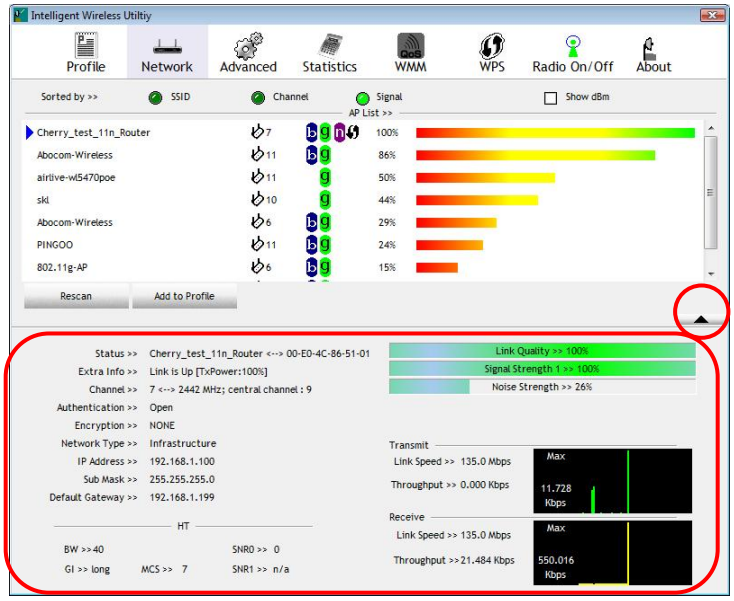
	This tab will show up if you select the AP that support 11n mode. Here shows the connected AP 802.11n related information.

Link Status

Click the triangle button at the right down corner of the windows to expand the link status. The link status page displays the detail information of current connection.

Click this button to show the information of Status Section.

Click this button to hide the information of Status Section.

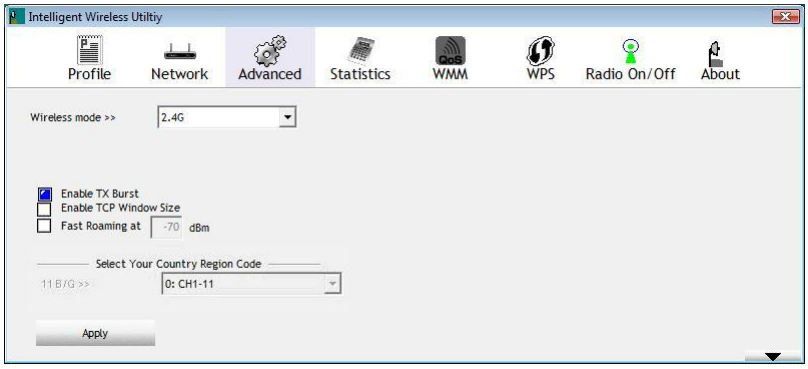


Link Status Tab	
Status	Shows the current connected AP SSID and MAC address. If there is no connection existing, it will show Disconnected.
Extra Info	Shows the link status and Tx power percentage.
Channel	Shows the current channel in use.
Authentication	Authentication mode used within the network, including Unknown, Open, WPA-PSK, WPA2-PSK, WPA and WPA2.
Encryption	Shows the encryption type currently in use. Valid value includes WEP, TKIP, AES, and Not Use.
Network Type	Network type in use, Infrastructure for BSS, Ad-Hoc for IBSS network.
IP Address	Shows the IP address information.
Sub Mask	Shows the Subnet Mask information.
Default Gateway	Shows the default gateway information.
Link Quality	Shows the connection quality based on signal strength and TX/RX packet error rate.
Signal Strength 1	Shows the Receiving signal strength, you can choose to display as percentage or dBm format.
Noise Strength	Shows the noise signal strength in the wireless environment.

Transmit	Shows the current Link Speed and Throughput of the transmit rate.
Receive	Shows the current Link Speed and Throughput of receive rate.
Link Speed	Shows the current transmitting rate and receiving rate.
Throughput	Shows the transmitting and receiving speed of data.

Advanced

This Advanced page provides advanced and detailed settings for your wireless network.

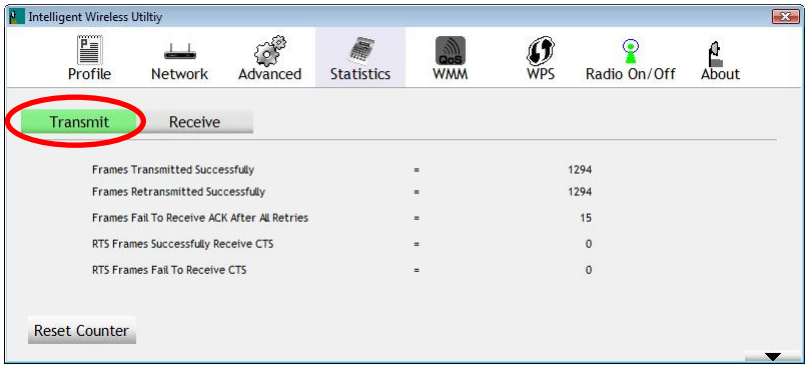


Advanced Tab	
Wireless mode	Here supports 2.4G (included 802.11b/g/n) wireless mode.
Enable TX Burst	Check to enable this function. This function enables the adapter to deliver better throughput during a period of

	time, it only takes effect when connecting with the AP that supports this function.
Enable TCP Window Size	Check to increase the transmission quality. The large TCP window size the better performance.
Fast Roaming at	Check to set the roaming interval, fast to roaming, setup by transmits power.
Apply	Click to apply above settings.

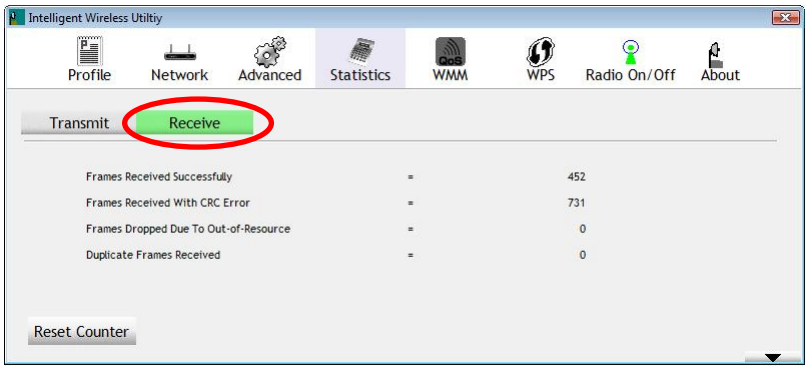
Statistics

The Statistics screen displays the statistics on your current network settings.



Transmit Statistics Tab	
Frames Transmitted Successfully	Shows information of frames successfully sent.
Frames Retransmitted Successfully	Shows information of frames successfully sent with one or more reties.
Frames Fail To Receive ACK After All Retries	Shows information of frames failed

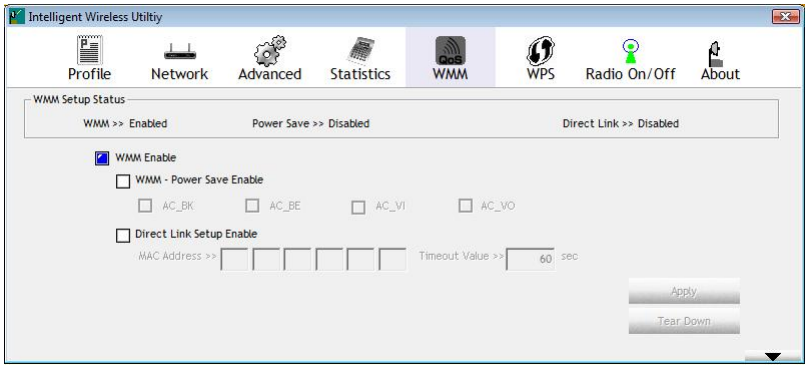
	transmit after hitting retry limit.
RTS Frames Successfully Receive CTS	Shows information of successfully receive CTS after sending RTS frame
RTS Frames Fail To Receive CTS	Shows information of failed to receive CTS after sending RTS.
Reset Counter	Click this button to reset counters to zero.



Receive Statistics Tab	
Frames Received Successfully	Shows information of frames Received Successfully.
Frames Received With CRC Error	Shows information of frames received with CRC error.
Frames Dropped Due To Out-of-Resource	Shows information of frames dropped due to resource issue.
Duplicate Frames Received	Shows information of frames received more than twice.
Reset Counter	Click this button to reset counters to zero.

WMM / QoS

The WMM page shows the Wi-Fi Multi-Media power save function and Direct Link Setup that ensure your wireless network quality.

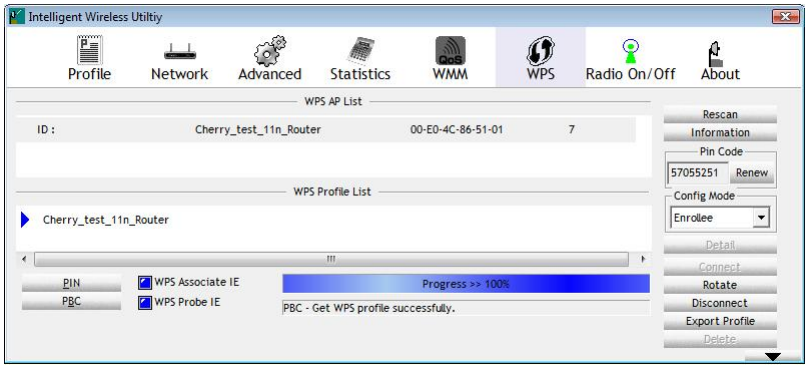


WMM/QoS Tab	
WMM Enable	Check the box to enable Wi-Fi Multi-Media function that is meant to improve audio, video and voice applications transmitted over Wi-Fi.
WMM- Power Save Enable	Select which ACs you want to enable the power saving mode. AC_BK (Access Category Background) AC_BE (Access Category Best Effort) AC_VI (Access Category Video) AC_VO (Access Category Voice)
Direct Link Setup Enable	Check the box to enable Direct Link Setup.
MAC Address	The setting of DLS(Direct Link Setup) indicates as follow: Fill in the blanks of Direct Link with MAC Address of STA, and the STA must conform to two conditions: • Connecting with the same AP that supports DLS feature.

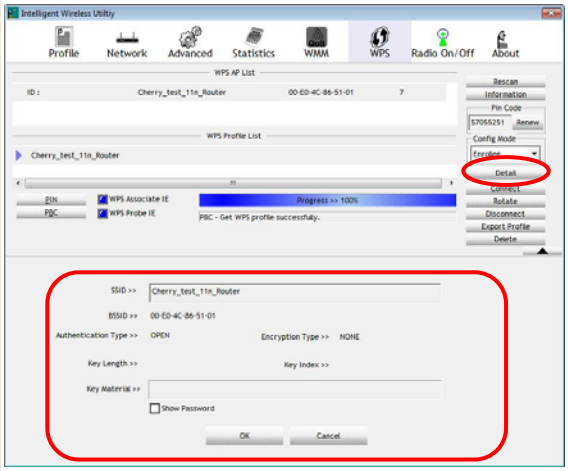
	• DLS enabled.
Timeout Value	Timeout Value represents that it disconnect automatically after few seconds. The value is integer that must be between 0~65535. It represents that it always connects if the value is zero. Default value of Timeout Value is 60 seconds.
Apply	Click this button to apply the settings.
Tear Down	Select a direct link STA, then click "Tear Down" button to disconnect the STA.

WPS

The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simplify the security setup and management of Wi-Fi networks. The STA as an Enrollee or external Registrar supports the configuration setup using PIN (Personal Identification Number) configuration method or PBC (Push Button Configuration) method through an internal or external Registrar.



WPS Tab	
WPS AP List	Display the information of surrounding APs with WPS IE from last scan result. List information included SSID,

	BSSID, Channel, ID (Device Password ID), Security-Enabled.
Rescan	Issue a rescan command to wireless NIC to update information on surrounding wireless network.
Information	Display the information about WPS IE on the selected network. List information included Authentication Type, Encryption Type, Config Methods, Device Password ID, Selected Registrar, State, Version, AP Setup Locked, UUID-E and RF Bands.
PIN Code	8-digit numbers. It is required to enter PIN Code into Registrar when using PIN method. When STA is Enrollee, you can use "Renew" button to re-generate new PIN Code.
Config Mode	Select from the pull-down menu to decide the station role-playing as an Enrollee or an external Registrar.
Detail	Click the Detail button to show the information about Security and Key in the credential. 

	If you select the AP that listed in the WPS Profile List field, you can click the **Detail** button to see more AP information. **SSID**: Shows the connected AP network name. **BSSID**: The MAC address of the connected AP. Fixed and cannot be changed. **Authentication Type**: The authentication type support Open, WPA-PSK and WPA2-PSK. **Encryption Type:** For **Open** authentication mode, the selection of encryption type are **NONE** and **WEP**. For **WPA-PSK** and **WPA2-PSK** authentication mode, the encryption type supports both **TKIP** and **AES**. **Key Length:** Only valid when using **Open** authentication mode and **WEP** encryption. There are key lengths 5, 10, 13 and 26. **Key Index:** Only valid when using **Open** authentication mode and **WEP** encryption. There are 1~4 key index. **Key Material:** The key material can be used to ensure the security of your wireless network. Fill in the appropriate value or phrase in **Key Material** field. **Show Password**: Check this box to show the passwords that have been entered. **OK**: Click to save and apply the new settings. **Cancel**: Click to leave and discard the settings.
Connect	Command to connect to the selected network inside credentials. The active selected credential is as like as the active selected Profile.
Rotate	Command to rotate to connect to the next network inside credentials.
Disconnect	Stop WPS action and disconnect this active link. And

	then select the last profile at the Profile Page. If there is an empty profile page, the driver will select any non-security AP.
Export Profile	Export all credentials to Profile.
Delete	Delete an existing credential. And then select the next credential if exist. If there is an empty credential, the driver will select any non-security AP.
PIN	Start to add to Registrar using PIN (Personal Identification Number) configuration method. If STA Registrar, remember that enter PIN Code read from your Enrollee before starting PIN.
PBC	Start to add to AP using PBC (Push Button Configuration) method.
WPS Associate IE	Send the association request with WPS IE during WPS setup. It is optional for STA.
WPS Probe IE	Send the probe request with WPS IE during WPS setup. It is optional for STA.
Progress Bar	Display rate of progress from Start to Connected status.
Status Bar	Display currently WPS Status.

Radio On/Off

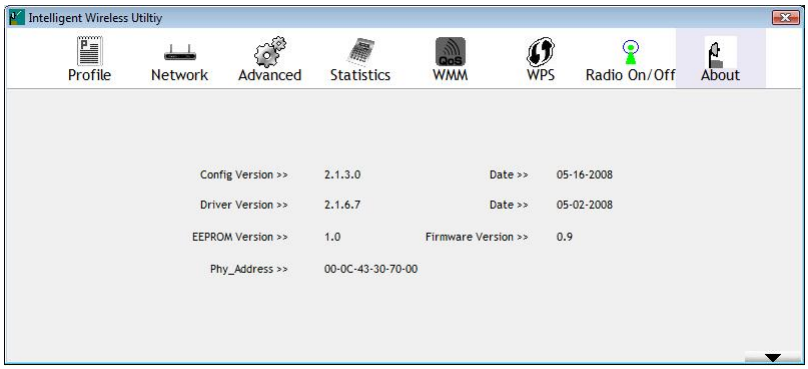
Click this button to turn on or off radio function.

This icon shows radio on, click to turn it off.

This icon shows radio off, click to turn it on.

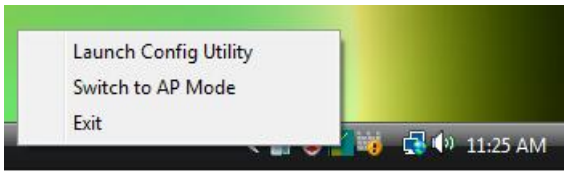
About

This page displays the information of the wireless card including, RaConfig Version/ Date, Driver Version/ Date, EEPROM Version and Phy_Address.



Utility Menu List

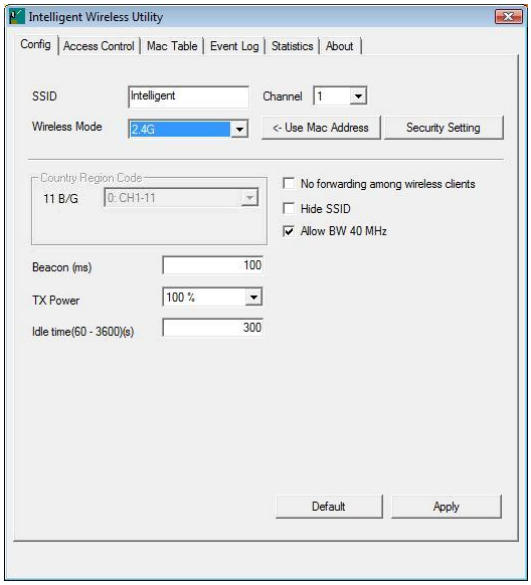
To access Windows Vista utility menu list, please right click the utility icon on the task bar.



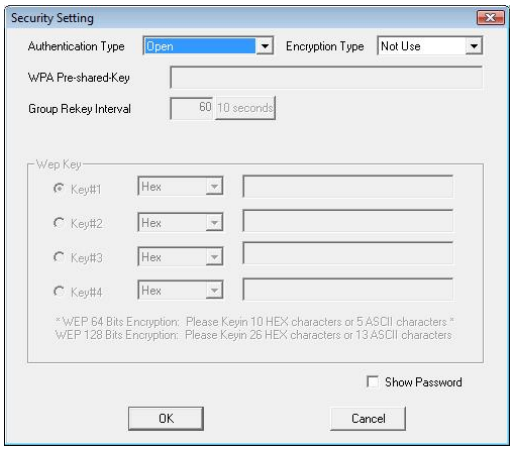
- **Launch Config Utility**: Select to open the utility screen.
- **Switch to AP Mode**: Select to make your wireless USB adapter act as a wireless AP.
- **Exit**: Select to close the utility program.

Soft AP mode

Config



Config	
SSID	AP name of user type. User also can click **Use Mac Address** button to display it.
Channel	Manually force the AP using the channel. The system default is CH 1.
Wireless mode	Here supports 2.4G (included 802.11b/g/n) wireless mode.
Use Mac Address	Click this button to replace SSID by MAC address.
Security Setting	Authentication mode and encryption algorithm used within the AP. The system default is no authentication and encryption.



Authentication Type: There are several types of authentication modes including Open, Shared, WPA-PSK, WPA2-PSK, and WPA-PSK/WPA2-PSK.

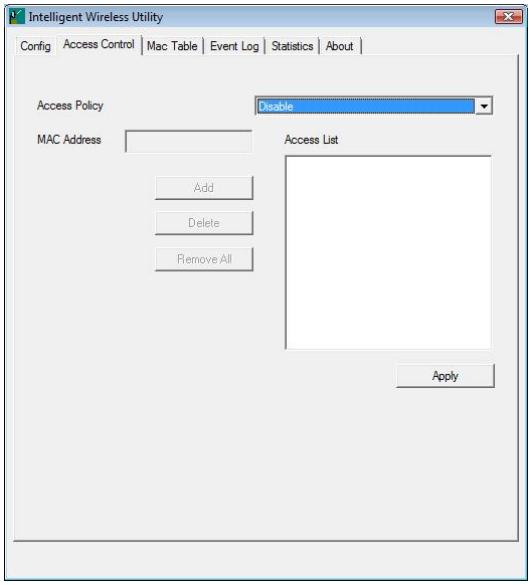
Encryption Type: For **Open** and **Shared** authentication mode, the selections of encryption type are **Not Use** and **WEP**. For **WPA-PSK, WPA2-PSK**, and **WPA-PSK/ WPA2-PSK** authentication mode, the encryption type supports both **TKIP** and **AES**.

WPA Pre-shared Key: This is the shared secret between AP and STA. For WPA-PSK and WPA2-PSK and WPA-PSK/ WPA2-PSK authentication mode, this field must be filled with character longer than 8 and less than 64 lengths.

Group Re-key Interval: Only valid when using WPA-PSK, WPA2-PSK, and WPA-PSK/ WPA2-PSK authentication mode to renew key. User can set to change by seconds or packets. Default is 600 seconds.

	WEP Key: Only valid when using WEP encryption algorithm. The key must match with the AP's key. There are several formats to enter the keys. • Hexadecimal (64bits): 10 Hex characters. • Hexadecimal (128bits): 26 Hex characters. • ASCII (64bits): 5 ASCII characters. • ASCII (128bits): 13 ASCII characters. **Show Password**: Check this box to show the password you entered.
Beacon (ms)	The time between two beacons. The system default is 100 ms.
TX Power	Manually force the AP transmits power from the pull down list 100%, 75%, 50%, 25% and Lowest. The system default is 100%.
Idle time(60-3600)(s)	It represents that the AP will idle after few seconds. The time must be set between 60~3600 seconds. Default value of idle time is 300 seconds.
No forwarding among wireless clients	No beacon among wireless client, clients can share information each other. The system default is no forwarding.
Hide SSID	Do not display AP name. System default no hide.
Allow BW 40MHz	Click to disable this function. Default is enabling.
Default	Use the system default value.
Apply	Click to apply the above settings.

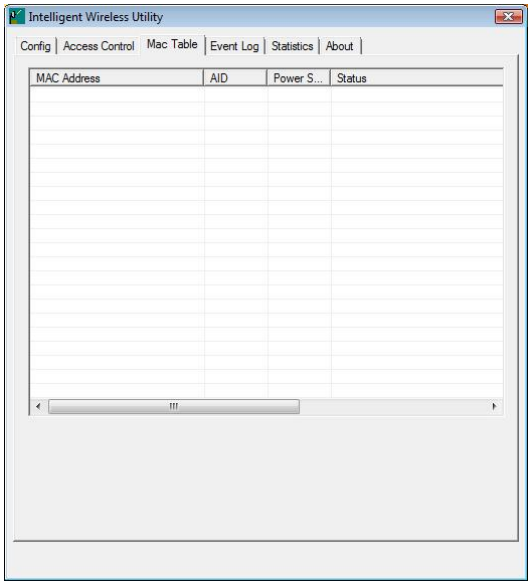
Access Control



Access Control	
Access Policy	User chooses whether AP start the function or not. System default is Disable. ● **Disable:** Do not use this access control function. ● **Allow All:** Only the MAC address listed in the Access List can connect with this soft AP. ● **Reject All:** Only the MAC address listed in the Access List can NOT connect with this soft AP.
MAC Address	Manually force the Mac address using the function. Click Add and the MAC address will be listed in the Access List pool.
Access List	Display all MAC Address that you have set.

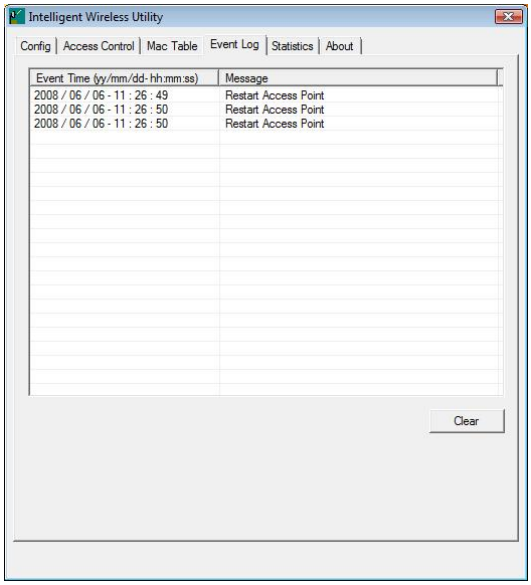
Add	Add the MAC address that you would like to set.
Delete	Delete the MAC address that you have set.
Remove All	Remove all MAC address in the Access List.
Apply	Apply the above changes.

MAC Table



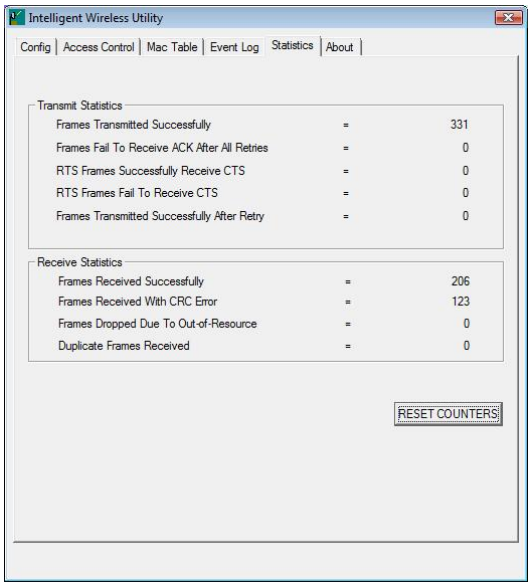
MAC Table	
MAC Address	The station MAC address of current connection.
AID	Raise value by current connection.
Power Saving Mode	The station of current connect whether it have to support.
Status	The status of current connection.

Event Log



Event Log	
Event Time (yy/mm/dd-hh:mm:ss)	Records the event time.
Message	Records all the event messages.

Statistics

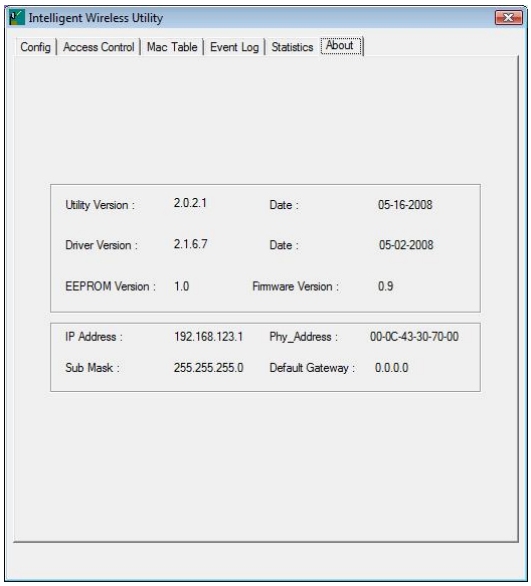

Intelligent Wireless Utility
Config
Access Control
Mac Table
Event Log
Statistics
About
Transmit Statistics
Frames Transmitted Successfully = 331
Frames Fail To Receive ACK After All Retries = 0
RTS Frames Successfully Receive CTS = 0
RTS Frames Fail To Receive CTS = 0
Frames Transmitted Successfully After Retry = 0
Receive Statistics
Frames Received Successfully = 206
Frames Received With CRC Error = 123
Frames Dropped Due To Out-of-Resource = 0
Duplicate Frames Received = 0
RESET COUNTERS

Transmit Statistics	
Frames Transmitted Successfully	Frames successfully sent.
Frames Fail To Receive ACK After All Retries	Frames failed transmit after hitting retry limit.
RTS Frames Successfully Receive CTS	Successfully receive CTS after sending RTS frame
RTS Frames Fail To Receive CTS	Failed to receive CTS after sending RTS.
Frames Transmitted Successfully After Retry	Frames successfully sent with one or more reties.

Receive Statistics	
Frames Received Successfully	Frames Received Successfully
Frames Received With CRC Error	Frames received with CRC error.
Frames Dropped Due To Out-of-Resource	Frames dropped due to resource issue
Duplicate Frames Received	Duplicate received frames.
Reset Counter	Reset counters to zero.

About

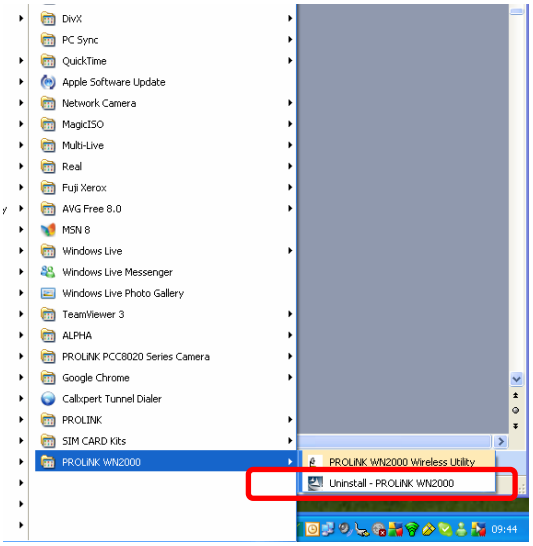
This page displays the wireless card and driver version information.


Intelligent Wireless Utility
Config
Access Control
Mac Table
Event Log
Statistics
About
Utility Version : 2.0.2.1 Date : 05-16-2008
Driver Version : 2.1.6.7 Date : 05-02-2008
EEPROM Version : 1.0 Firmware Version : 0.9
IP Address : 192.168.123.1 Phy_Address : 00-0C-43-30-70-00
Sub Mask : 255.255.255.0 Default Gateway : 0.0.0.0

UNINSTALLATION FOR WINDOWS 2000/XP

In case you need to uninstall the Utility and driver, please refer to below steps. (As you uninstall the utility, the driver will be uninstalled as well.)

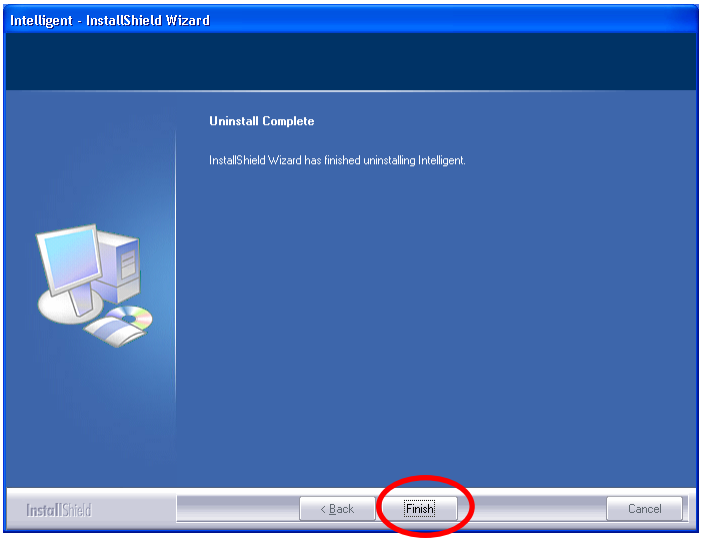
1. Go to **Start →All Programs →PROLiNK WN2000 → Uninstall –PROLiNK WN2000.**



2. Click **Yes** to complete remove the selected application and all of its features.

Intelligent - InstallShield Wizard
Do you want to completely remove the selected application and all of its features?
Yes
No

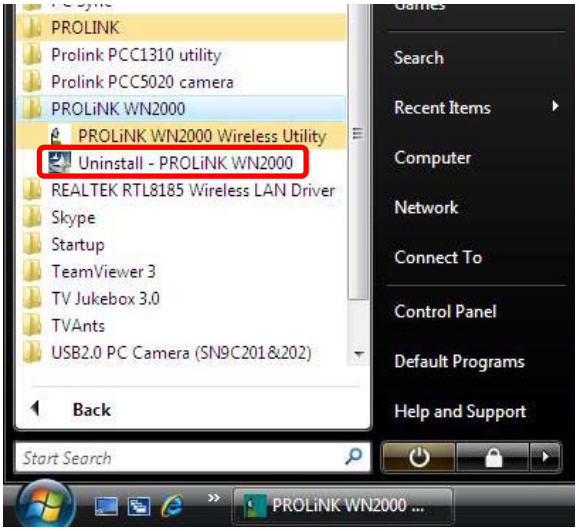
3. Then click **Finish** to complete the uninstallation.



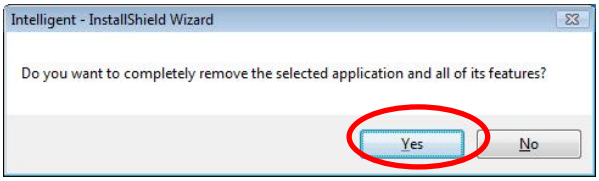
UNINSTALLATION FOR WINDOWS VISTA

In case you need to uninstall the utility and driver, please refer to below steps. (As you uninstall the utility, the driver will be uninstalled as well.)

1. Go to **Start → Programs →PROLiNK WN2000 → Uninstall –PROLiNK WN2000.**



2. Click **Yes** to complete remove the selected application and all of its features.


Intelligent - InstallShield Wizard
Do you want to completely remove the selected application and all of its features?
Yes
No

3. Then click **Finish** to complete the uninstallation.